Journal of Number Theory 130 (2010) 1854–1875

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Reciprocal relations between cyclotomic fields

Charles Helou

Penn State Univ., 25 Yearsley Mill Rd, Media, PA 19063, United States

ARTICLE INFO

Article history:
Received 17 August 2009
Revised 2 November 2009
Available online 31 March 2010
Communicated by David Goss

MSC:
11R18

Keywords:
Cyclotomic fields
Norms
Prime ideal factorization
Cyclotomic polynomials

ABSTRACT

We describe a reciprocity relation between the prime ideal factorization, and related properties, of certain cyclotomic integers of the type $\phi_n(c-\zeta_m)$ in the cyclotomic field of the m-th roots of unity and that of the symmetrical elements $\phi_m(c-\zeta_n)$ in the cyclotomic field of the n-th roots. Here m and n are two positive integers, ϕ_n is the n-th cyclotomic polynomial, ζ_m a primitive m-th root of unity, and c a rational integer. In particular, one of these integers is a prime element in one cyclotomic field if and only if its symmetrical counterpart is prime in the other cyclotomic field. More properties are also established for the special class of pairs of cyclotomic integers $(1-\zeta_p)^q-1$ and $(1-\zeta_q)^p-1$, where p and q are prime numbers.

1. Introduction

Let m, n denote positive integers, ζ_n a primitive n-th root of unity in an algebraically closed field containing the rational number field $\mathbb{Q}$ such that if $m \mid n$, then $\zeta_m = \zeta_n^{n/m}$. The element $\lambda_n = 1-\zeta_n$ of the cyclotomic field $K_n = \mathbb{Q}(\zeta_n)$ plays a special role in the sequel. If n is a prime power, λ_n is a prime element of the ring $O_n = \mathbb{Z}[\zeta_n]$ of integers of K_n, and if n is divisible by two distinct prime numbers, λ_n is a unit of O_n [W]. In particular if $n = p$ is a prime number, then $\lambda_p O_p$ is the only prime ideal of O_p above p, and the integral elements $1-\lambda_p^n$ $(n \geqslant 1)$, form a topological basis for the group of principal units in the λ_p-adic completion $\hat{K}_p$ of K_p [H]. Due to this property, the elements $1-\lambda_p^n$ are often used to establish explicit expressions for the norm residue symbol $(\cdot,\cdot)_{\hat{K}_p}$ in the local field $\hat{K}_p$, which in turn lead to explicit reciprocity laws for the power residue symbol $(\frac{\cdot}{\cdot})_{p,K_p}$ in the global field K_p, via the relation $(\frac{\alpha}{\beta})_{p,K_p}(\frac{\beta}{\alpha})_{p,K_p}^{-1} = (\beta,\alpha)_{\hat{K}_p}$, for relatively prime elements $\alpha, \beta \in O_p$ not divisible by λ_p and for $p \geqslant 3$ [AT]. This justifies the interest in the study of the elements $1-\lambda_p^n$ as

E-mail address: cxh22@psu.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.01.015

global objects in K_p, and in particular of their prime ideal factorization in O_p. For two prime numbers p and q, there is a reciprocal relation, a kind of symmetry, between the factorization of $(1-\lambda_p^q)$ in K_p and that of $(1-\lambda_q^p)$ in K_q. To generalize this property from K_p to K_m, since $1-\lambda_p^q=\zeta_p\phi_q(\lambda_p)$, one is lead to consider the elements $\phi_n(\lambda_m)=\phi_n(1-\zeta_m)$ or more generally $\phi_n(c-\zeta_m)$, with $c\in\mathbb{Z}$, where ϕ_n is the n-th cyclotomic polynomial over $\mathbb{Q}$. A natural starting point is the study of the rational integers $N_m(\phi_n(c-\zeta_m))$ and $N_m(\lambda_m^n-1)$, where N_m is the norm map in $K_m|\mathbb{Q}$. They generalize the Mersenne numbers $2^p-1=N_p(\lambda_p^2-1)$ for primes p, and the Fermat numbers $2^{2^k}+1=N_{2^{k+1}}(\lambda_{2^{k+1}}^2-1)$ for positive integers k. Several identities and relations between such norms are established before turning to their arithmetical properties, and in particular investigating their prime factors. We thus have

Theorem 1. *For any positive integers m, n and any rational number $c\in\mathbb{Q}$,*

$$N_m\big(\phi_n(c-\zeta_m)\big)=N_n\big(\phi_m(c-\zeta_n)\big),$$

where $N_m=N_{\mathbb{Q}(\zeta_m)|\mathbb{Q}}$ is the norm map in $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ and ϕ_m is the m-th cyclotomic polynomial, and similarly for N_n and ϕ_n.

In particular, $N_p(\lambda_p^q-1)=N_q(\lambda_q^p-1)$ for any prime numbers p, q. There are several other variations and extensions of such identities.

On the other hand, $N_{p^h}(1-\lambda_{p^h}^n)\equiv 1 \pmod{p^{\lceil\frac{n}{\varphi(p^h)}\rceil}}$ for positive integers h, n and prime p, where φ is Euler's function, and $\lceil x\rceil$, for a real number x, is the smallest integer $\geqslant x$. In particular, $N_p(1-\lambda_p^q)=N_q(1-\lambda_q^p)\equiv 1 \pmod{p^{\lceil\frac{q}{p-1}\rceil}q^{\lceil\frac{p}{q-1}\rceil}}$ for any distinct odd prime numbers p, q. Another key theorem is

Theorem 2. *For any positive integers m, n, and any element x of the ring of integers O_m of $K_m=\mathbb{Q}(\zeta_m)$, if a prime number l divides the norm $N_m(\phi_n(x))$ and does not divide mn, then the order f_n of l modulo n divides the order f_m of l modulo m.*

We deduce from it, among other results, an essential corollary, namely if the prime number l divides $N_m(\phi_n(c-\zeta_m))=N_n(\phi_m(c-\zeta_n))$, with $c\in\mathbb{Z}$, and if $l\nmid mn$, then the orders of l modulo m and modulo n are equal. In particular, if l, p, q are prime numbers such that l divides $N_p(\lambda_p^q-1)=N_q(\lambda_q^p-1)$, then l has the same order modulo p and modulo q. Furthermore, we establish

Theorem 3. *For any positive integer n and any $c\in\mathbb{Z}$ such that $\phi_n(c)$ and n have no common factor, $\phi_n(c)$ is a rational prime if and only if $(c-\zeta_n)O_n$ is a prime ideal of O_n, and in this case, the prime $\phi_n(c)$ splits completely in $K_n|\mathbb{Q}$.*

This applies in particular to the Mersenne numbers $M_p=2^p-1=\phi_p(2)$, for any prime number p, and to the Fermat numbers $F_k=2^{2^k}+1=\phi_{2^{k+1}}(2)$, for any positive integer k. The main result is the following one about prime ideal factorization.

Theorem 4. *Let m, n be two positive integers and $c\in\mathbb{Z}$ such that $N_m(\phi_n(c-\zeta_m))$ is relatively prime to mn. Let $|N_m(\phi_n(c-\zeta_m))|=|N_n(\phi_m(c-\zeta_n))|=\prod_{i=1}^r l_i^{h_i}$, where $l_1,\dots,l_r$ are distinct prime numbers and $h_1,\dots,h_r$ are positive integers. For $1\leqslant i\leqslant r$, let f_i be the common order of l_i modulo m and modulo n (it is proved before Theorem 4 that f_i divides h_i) and $m_i=\frac{h_i}{f_i}$. For every i, let $\mathfrak{l}_i$ (resp. $\mathfrak{l}_i'$) be a prime ideal of O_m (resp. O_n) dividing l_i and $\phi_n(c-\zeta_m)$ (resp. dividing l_i and $\phi_m(c-\zeta_n)$). Then*

$$\phi_n(c-\zeta_m)O_m=\prod_{i=1}^r \mathfrak{l}_{i,1}\dots\mathfrak{l}_{i,m_i},$$

and

$$\phi_m(c-\zeta_n)O_n = \prod_{i=1}^{r} \mathfrak{l}'_{i,1}\dots\mathfrak{l}'_{i,m_i},$$

where $\mathfrak{l}_{i,1},\dots,\mathfrak{l}_{i,m_i}$ *(resp.* $\mathfrak{l}'_{i,1},\dots,\mathfrak{l}'_{i,m_i}$*) are* m_i*, not necessarily distinct, prime ideal conjugates of* $\mathfrak{l}_i$ *in* O_m *(resp. of* $\mathfrak{l}'_i$ *in* O_n*), for every* $1\leqslant i\leqslant r$.

In particular, if, in Theorem 4, $h_i = f_i$ for $1\leqslant i\leqslant r$, then, for every i, there exists a unique prime ideal $\mathfrak{l}_i$ of O_m (resp. $\mathfrak{l}'_i$ of O_n) dividing l_i and $\phi_n(c-\zeta_m)$ (resp. dividing l_i and $\phi_m(c-\zeta_n)$), and we have $\phi_n(c-\zeta_m)O_m = \prod_{i=1}^{r}\mathfrak{l}_i$ and $\phi_m(c-\zeta_n)O_n = \prod_{i=1}^{r}\mathfrak{l}'_i$. This yields the following reciprocity property.

Theorem 5. *For two positive integers* m, n *and* $c\in\mathbb{Z}$ *such that* mn *and* $N_m(\phi_n(c-\zeta_m))$ *are relatively prime,* $\phi_n(c-\zeta_m)O_m$ *is a prime ideal of* O_m *if and only if* $\phi_m(c-\zeta_n)O_n$ *is a prime ideal of* O_n*. This is also equivalent to the condition*: $N_m(\phi_n(c-\zeta_m)) = N_n(\phi_m(c-\zeta_n)) = l^f$ *for some prime number* l *whose order modulo* m *and modulo* n *is* f.

The same results, as in Theorems 4 and 5, hold with m, n replaced by prime numbers p, q respectively, and $\phi_n(c-\zeta_m)$ (resp. $\phi_m(c-\zeta_n)$) replaced by $1-\lambda_p^q$ (resp. $1-\lambda_q^p$), giving similar prime ideal factorizations for $(1-\lambda_p^q)$ in K_p and for $(1-\lambda_q^p)$ in K_q. In particular, $1-\lambda_p^q$ is a prime element of O_p if and only if $1-\lambda_q^p$ is a prime element of O_q (Theorem 6).

A plausible conjecture, based on the available numerical evidence, is that if p and q are two distinct prime numbers, then every prime number l dividing $N_p(\lambda_p^q-1) = N_q(\lambda_q^p-1)$ satisfies $l\equiv 1 \pmod{pq}$. Here, we are able to prove that for such prime divisors l, the common order f of l modulo the distinct primes p and q is an odd integer (Corollary 2 to Proposition 8). Also, if $q=3$ and $p\geqslant 5$, then this conjectured property holds (Corollary 1 to Proposition 8). Moreover (Corollary 2 to Proposition 10):

For a prime $p\geqslant 5$, if $N_p(\lambda_p^3-1) = N_3(\lambda_3^p-1) = \prod_{i=1}^{r} l_i^{m_i}$ is the rational prime factorization of the norm, with distinct prime numbers l_i and positive integers m_i, then for every $1\leqslant i\leqslant r$, there exists a unique prime ideal $\mathfrak{l}_i$ of O_p (resp. $\mathfrak{l}'_i$ of O_3) dividing l_i and $1-\lambda_p^3$ (resp. dividing l_i and $1-\lambda_3^p$), and we have the similar prime ideal factorizations $(1-\lambda_p^3)O_p = \prod_{i=1}^{r}\mathfrak{l}_i^{m_i}$ and $(1-\lambda_3^p)O_3 = \prod_{i=1}^{r}\mathfrak{l}'^{m_i}_i$.

Part of the results had been presented in [He], but they are here substantially extended and completed.

2. Identities between norms of cyclotomic elements

The set of natural numbers $0,1,2,\dots$ is denoted by $\mathbb{N}$, the ring of rational integers by $\mathbb{Z}$, and the fields of rational numbers, real numbers and complex numbers by $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ respectively.

For a positive integer n, let ζ_n be a primitive n-th root of unity in $\mathbb{C}$, and $K_n = \mathbb{Q}(\zeta_n)$ the n-th cyclotomic field, $O_n = \mathbb{Z}[\zeta_n]$ its ring of integers, N_n the norm map in $K_n|\mathbb{Q}$. Let ϕ_n be the n-th cyclotomic polynomial, i.e. the irreducible polynomial of ζ_n over $\mathbb{Q}$, given by $\phi_n(X) = \prod_{k\in R_n^*}(X-\zeta_n^k)$, where $R_n^* = \{k\in\mathbb{N}:\ 1\leqslant k\leqslant n,\ \gcd(k,n)=1\}$ is the standard reduced residue system modulo n. Let $G_n = Gal(K_n|\mathbb{Q}) = \{\sigma_k^{(n)}:\ k\in R_n^*\}$ be the Galois group of $K_n|\mathbb{Q}$, consisting of the $\mathbb{Q}$-automorphisms $\sigma_k^{(n)}$ of K_n defined, for any integer k relatively prime to n, by $\sigma_k^{(n)}(\zeta_n) = \zeta_n^k$. The group G_n is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ of invertible residue classes modulo n. The degree of $K_n|\mathbb{Q}$ is the cardinality $|R_n^*| = |(\mathbb{Z}/n\mathbb{Z})^*|$, i.e. $[K_n:\mathbb{Q}] = \varphi(n)$, where φ is Euler's totient function. We also set $\lambda_n = 1-\zeta_n$. In the sequel we assume that if a positive integer m divides n, then $\zeta_m = \zeta_n^{n/m}$, e.g. by setting $\zeta_n = \exp(\frac{2i\pi}{n})$ for every n.

For an element $x\in K_n$, the field polynomial of x in $K_n|\mathbb{Q}$, which is the same as the norm of $X-x$ in the function field extension $K_n(X)|\mathbb{Q}(X)$ [ZS], is defined by $P_{x,K_n|\mathbb{Q}}(X) = \mathcal{N}_n(X-x) = \prod_{k\in R_n^*}(X-\sigma_k^{(n)}(x))$. For $z\in\mathbb{C}$, the complex number $P_{x,K_n|\mathbb{Q}}(z) = \prod_{k\in R_n^*}(z-\sigma_k^{(n)}(x))$, obtained by substituting z for X in $P_{x,K_n|\mathbb{Q}}(X) = \mathcal{N}_n(X-x)$ will also be written $\mathcal{N}_n(z-x)$. Thus, if $x = g(\zeta_n)$, where $g\in\mathbb{Q}(x)$ is a rational fraction with rational coefficients, then $\mathcal{N}_n(z-g(\zeta_n)) = \prod_{k\in R_n^*}(z-g(\zeta_n^k))$.

Lemma 1. *For any rational fractions $f, g \in \mathbb{Q}(X)$ and any positive integers m, n, we have*

$$N_m\big(\mathcal{N}_n\big(f(\zeta_m) - g(\zeta_n)\big)\big) = (-1)^{\varphi(m)\varphi(n)} N_n\big(\mathcal{N}_m\big(g(\zeta_n) - f(\zeta_m)\big)\big) = \prod_{\substack{j\in R_m^* \\ k\in R_n^*}} \big(f\big(\zeta_m^j\big) - g\big(\zeta_n^k\big)\big).$$

Proof. By definition, $\mathcal{N}_n(f(\zeta_m) - g(\zeta_n)) = \prod_{k\in R_n^*}(f(\zeta_m) - g(\zeta_n^k))$ and it lies in K_m, since $\mathcal{N}_n(X - g(\zeta_n))$ has its coefficients invariant under the action of the Galois group G_n and therefore lies in $\mathbb{Q}(X)$. Then

$$\begin{aligned} N_m\big(\mathcal{N}_n\big(f(\zeta_m) - g(\zeta_n)\big)\big) &= \prod_{j\in R_m^*} \sigma_j^{(m)}\big(\mathcal{N}_n\big(f(\zeta_m) - g(\zeta_n)\big)\big) = \prod_{j\in R_m^*} \mathcal{N}_n\big(f\big(\zeta_m^j\big) - g(\zeta_n)\big) \\ &= \prod_{j\in R_m^*}\prod_{k\in R_n^*} \big(f\big(\zeta_m^j\big) - g\big(\zeta_n^k\big)\big) = \prod_{\substack{j\in R_m^* \\ k\in R_n^*}} \big(f\big(\zeta_m^j\big) - g\big(\zeta_n^k\big)\big). \end{aligned}$$

Similarly, by exchange of m and n, we have

$$N_n\big(\mathcal{N}_m\big(g(\zeta_n) - f(\zeta_m)\big)\big) = \prod_{k\in R_n^*}\prod_{j\in R_m^*} \big(g\big(\zeta_n^k\big) - f\big(\zeta_m^j\big)\big) = \prod_{\substack{j\in R_m^* \\ k\in R_n^*}} \big(g\big(\zeta_n^k\big) - f\big(\zeta_m^j\big)\big).$$

Hence

$$\begin{aligned} N_m\big(\mathcal{N}_n\big(f(\zeta_m) - g(\zeta_n)\big)\big) &= \prod_{j\in R_m^*}\prod_{k\in R_n^*} \big(f\big(\zeta_m^j - g\big(\zeta_n^k\big)\big)\big) = \prod_{j\in R_m^*} (-1)^{\varphi(n)} \prod_{k\in R_n^*} \big(g\big(\zeta_n^k\big) - f\big(\zeta_m^j\big)\big) \\ &= (-1)^{\varphi(m)\varphi(n)} \prod_{j\in R_m^*}\prod_{k\in R_n^*} \big(g\big(\zeta_n^k\big) - f\big(\zeta_m^j\big)\big) \\ &= (-1)^{\varphi(m)\varphi(n)} N_n\big(\mathcal{N}_m\big(g(\zeta_n) - f(\zeta_m)\big)\big). \qquad \square \end{aligned}$$

Remark 1. If the positive integers m and n are relatively prime, then the field extensions $K_m|\mathbb{Q}$ and $K_n|\mathbb{Q}$ are linearly disjoint, with compositum $K_mK_n = K_{mn}$, and Galois group isomorphisms $Gal(K_{mn}|K_m) \simeq G_n$ and $Gal(K_{mn}|K_n) \simeq G_m$, so that the equalities in Lemma 1 amount to the transitivity relation

$$N_m\big(N_{K_{mn}|K_m}\big(f(\zeta_m) - g(\zeta_n)\big)\big) = N_n\big(N_{K_{mn}|K_n}\big(f(\zeta_m) - g(\zeta_n)\big)\big) = N_{mn}\big(f(\zeta_m) - g(\zeta_n)\big).$$

Theorem 1. *For any positive integers m, n, and any $c \in \mathbb{Q}$,*

$$N_m\big(\phi_n(c - \zeta_m)\big) = N_n\big(\phi_m(c - \zeta_n)\big) = \prod_{\substack{j\in R_m^* \\ k\in R_n^*}} \big(c - \zeta_m^j - \zeta_n^k\big).$$

And if m and n are relatively prime, $N_m(\phi_n(c - \zeta_m)) = N_n(\phi_m(c - \zeta_n)) = N_{mn}(c - \zeta_m - \zeta_n)$.

Proof. These follow from Lemma 1, by noting that $\mathcal{N}_n(c - \zeta_m - \zeta_n) = \prod_{k\in R_n^*}(c - \zeta_m - \zeta_n^k) = \phi_n(c - \zeta_m)$ and $\mathcal{N}_m(c - \zeta_m - \zeta_n) = \phi_m(c - \zeta_n)$, and from Remark 1 for the last equality. $\square$

Corollary. *For any positive integers m, n,*

$$N_m\big(\phi_n(\lambda_m)\big) = N_n\big(\phi_m(\lambda_n)\big).$$

Remark 2. From the definition, we have, for any $c \in \mathbb{Q}$,

$$N_m(c-\zeta_m) = \prod_{j\in R_m^*} \big(c-\zeta_m^j\big) = \phi_m(c). \tag{1}$$

Proposition 1. *For any positive integers m, n and any $c \in \mathbb{Q}$, we have*

$$N_m\big((c-\zeta_m)^n - 1\big) = \prod_{d|n} N_d\big(\phi_m(c-\zeta_d)\big).$$

Proof. Partitionning the n-th roots of unity in classes defined by their orders yields the well-known identity [W,IR] for cyclotomic polynomials $X^n - 1 = \prod_{d|n} \phi_d(X)$. Hence, for any $x \in K_m$,

$$N_m\big(x^n - 1\big) = \prod_{d|n} N_m\big(\phi_d(x)\big). \tag{2}$$

In particular, taking $x = c - \zeta_m$, and using Theorem 1 to substitute $N_m(\phi_d(c-\zeta_m)) = N_d(\phi_m(c-\zeta_d))$, the result follows. □

Corollary. *For any positive integers m, n,*

$$N_m\big(\lambda_m^n - 1\big) = \prod_{d|n} N_d\big(\phi_m(\lambda_d)\big).$$

In particular, for any $k \in \mathbb{N}$ and any prime number p,

$$N_{2^{k+1}}\big(\lambda_{2^{k+1}}^p - 1\big) = N_p\big(\lambda_p^{2^k} + 1\big).$$

Proof. These follow from Proposition 1, by taking $c = 1$ in the first part, and taking $m = 2^{k+1}$ and $n = p$ in the second part. Indeed, in the latter case, $N_{2^{k+1}}(\lambda_{2^{k+1}}^p - 1) = N_1(\phi_{2^{k+1}}(\lambda_1))N_p(\phi_{2^{k+1}}(\lambda_p))$, where $\phi_{2^{k+1}}(X) = X^{2^k} + 1$ and $\lambda_1 = 0$, while N_1 is the identity map of $\mathbb{Q}$, which yields the second formula. □

Proposition 2. *For any integer $m \geqslant 2$ and any prime number p, we have*

$$N_m\big(\lambda_m^p - 1\big) = N_m\big(\phi_p(\lambda_m)\big) = N_p\big(\phi_m(\lambda_p)\big).$$

Proof. Since $\phi_p(X) = \frac{X^p-1}{X-1}$, we have $N_m(\phi_p(\lambda_m)) = \frac{N_m(\lambda_m^p-1)}{N_m(-\zeta_m)}$. Moreover, $N_m(-\zeta_m) = (-1)^{\varphi(m)} N_m(\zeta_m)$, and $N_m(\zeta_m) = \prod_{j\in R_m^*} \zeta_m^j = \zeta_m^{\sum_{j\in R_m^*} j}$. If $m \geqslant 3$, the residues modulo m relatively prime to m can be partitioned in pairs $\{j, m-j\}$, with $1 \leqslant j < \frac{m}{2}$, so that $\varphi(m)$ is even, $\sum_{j\in R_m^*} j = \frac{\varphi(m)}{2} m$ is divisible by m, and therefore $\zeta_m^{\sum_{j\in R_m^*} j} = 1 = (-1)^{\varphi(m)}$. If $m = 2$, then $\sum_{j\in R_2^*} j = 1 = \varphi(2)$, and $\zeta_2^{\sum_{j\in R_2^*} j} = -1 = (-1)^{\varphi(2)}$. Thus

$$N_m(\zeta_m) = (-1)^{\varphi(m)} = \begin{cases} 1, & \text{if } m \geqslant 3, \\ -1, & \text{if } m = 2. \end{cases} \tag{3}$$

Hence $N_m(-\zeta_m) = 1$ and $N_m(\lambda_m^p - 1) = N_m(\phi_p(\lambda_m))$. The second equality follows from the corollary to Theorem 1. □

Corollary 1. *For any positive integer n and any prime number p,*

$$N_p\big(\lambda_p^n - 1\big) = \prod_{\substack{d|n \\ d\geqslant 2}} N_d\big(\lambda_d^p - 1\big).$$

Proof. By the corollary to Proposition 1, $N_p(\lambda_p^n - 1) = \prod_{d|n} N_d(\phi_p(\lambda_d))$. By Proposition 2, $N_d(\phi_p(\lambda_d)) = N_d(\lambda_d^p - 1)$ for $d \geqslant 2$ $(d \mid n)$, while for $d = 1$, trivially, $N_1(\phi_p(\lambda_1)) = \phi_p(0) = 1$. Hence the stated relation. □

Corollary 2. *For any prime numbers p and q,*

$$N_p\big(\lambda_p^q - 1\big) = N_q\big(\lambda_q^p - 1\big) = \prod_{\substack{1\leqslant j\leqslant p-1 \\ 1\leqslant k\leqslant q-1}} \big(1 - \zeta_p^j - \zeta_q^k\big).$$

And if $p \neq q$, then $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1) = N_{pq}(1 - \zeta_p - \zeta_q)$.

Proof. These equalities follow from Proposition 2 and Theorem 1. □

Proposition 3. *Let m and d be two positive integers such that d divides m and every prime divisor of m divides d. For any $c \in \mathbb{Q}$, we have*

$$N_m(c - \zeta_m) = \phi_d\big(c^{m/d}\big).$$

Proof. By (1), in Remark 2, $N_m(c - \zeta_m) = \phi_m(c)$. As d and m have the same prime factors, and d divides m, we have the classical relation $\phi_m(X) = \phi_d(X^{\frac{m}{d}})$ (see [L]). The result follows by substituting $X = c$. □

Corollary. *For any positive integers k, l, n such that $1 \leqslant l \leqslant k$, and for any $c \in \mathbb{Q}$,*

$$N_{n^k}(c - \zeta_{n^k}) = \phi_{n^l}\big(c^{n^{k-l}}\big) = \phi_n\big(c^{n^{k-1}}\big).$$

Remark 3. For any polynomial $f \in \mathbb{Q}[X]$ with rational coefficients, and any positive integer m,

$$N_m\big(f(\zeta_m)\big) = \prod_{j\in R_m^*} f\big(\zeta_m^j\big) = R(\phi_m, f)$$

is the resultant of the cyclotomic polynomial ϕ_m and the polynomial f [L]. In particular, for any positive integers m, n,

$$N_m\big(\phi_n(\zeta_m)\big) = R(\phi_m, \phi_n) = (-1)^{\varphi(m)\varphi(n)} R(\phi_n, \phi_m) = (-1)^{\varphi(m)\varphi(n)} N_n\big(\phi_m(\zeta_n)\big).$$

Proposition 4. *For any prime numbers p, q and any positive integers h, k,*

$$N_{p^h}\big(\lambda_{p^h}^{q^k}-1\big)=\prod_{i=1}^{k}N_{q^i}\big(\phi_{p^h}(\lambda_{q^i})\big).$$

Proof. By the corollary to Theorem 1, $N_{p^h}(\phi_{q^k}(\lambda_{p^h}))=N_{q^k}(\phi_{p^h}(\lambda_{q^k}))$. Since $\phi_{q^k}(X)=\frac{X^{q^k}-1}{X^{q^{k-1}}-1}$ (e.g. [L]), the previous relation implies that

$$N_{p^h}\big(\lambda_{p^h}^{q^k}-1\big)=N_{q^k}\big(\phi_{p^h}(\lambda_{q^k})\big)N_{p^h}\big(\lambda_{p^h}^{q^{k-1}}-1\big). \tag{4}$$

Similarly, $N_{p^h}(\lambda_{p^h}^{q^{k-1}}-1)=N_{q^{k-1}}(\phi_{p^h}(\lambda_{q^{k-1}}))N_{p^h}(\lambda_{p^h}^{q^{k-2}}-1)$, which when substituted in (4) gives

$$N_{p^h}\big(\lambda_{p^h}^{q^k}-1\big)=N_{q^k}\big(\phi_{p^h}(\lambda_{q^k})\big)N_{q^{k-1}}\big(\phi_{p^h}(\lambda_{q^{k-1}})\big)N_{p^h}\big(\lambda_{p^h}^{q^{k-2}}-1\big).$$

Repeated application of (4) and substitution in the expression for $N_{p^h}(\lambda_{p^h}^{q^k}-1)$ yield, for $1\leqslant j\leqslant k$, the relation

$$N_{p^h}\big(\lambda_{p^h}^{q^k}-1\big)=N_{p^h}\big(\lambda_{p^h}^{q^{k-j}}-1\big)\prod_{i=k-j+1}^{k}N_{q^i}\big(\phi_{p^h}(\lambda_{q^i})\big).$$

The result then follows by taking $j=k$ and using (3). □

Corollary 1. *For any prime numbers p, q and any positive integers h, k,*

$$\prod_{i=1}^{k}N_{q^i}\big(\lambda_{q^i}^{p^h}-1\big)=N_{p^h}\big(\lambda_{p^h}^{q^k}-1\big)\prod_{i=1}^{k}N_{q^i}\big(\lambda_{q^i}^{p^{h-1}}-1\big).$$

In particular,

$$\prod_{i=1}^{k}N_{q^i}\big(\lambda_{q^i}^{p}-1\big)=N_{p}\big(\lambda_{p}^{q^k}-1\big),$$

and

$$N_{q}\big(\lambda_{q}^{p^h}-1\big)=N_{p^h}\big(\lambda_{p^h}^{q}-1\big)N_{q}\big(\lambda_{q}^{p^{h-1}}-1\big).$$

Proof. The first relation results from Proposition 4, in view of the fact that $\phi_{p^h}(X)=\frac{X^{p^h}-1}{X^{p^{h-1}}-1}$, which allows the substitution $N_{q^i}(\phi_{p^h}(\lambda_{q^i}))=\frac{N_{q^i}(\lambda_{q^i}^{p^h}-1)}{N_{q^i}(\lambda_{q^i}^{p^{h-1}}-1)}$. The second relation is the case $h=1$ of the first one, taking into account that $N_{q^i}(\lambda_{q^i}-1)=N_{q^i}(-\zeta_{q^i})=1$, for $1\leqslant i\leqslant k$, by (3). The third relation is the case $k=1$ of the first one. □

Corollary 2. *For any prime number q and any positive integers h, k,*

$$N_{2^h}\big(\lambda_{2^h}^{q^k}-1\big)=\prod_{i=1}^{k}N_{q^i}\big(\lambda_{q^i}^{2^{h-1}}+1\big).$$

In particular,

$$\prod_{i=1}^{k}N_{q^i}(\lambda_{q^i}+1)=\prod_{i=1}^{k}N_{q^i}(2-\zeta_{q^i})=2^{q^k}-1.$$

Proof. The first relation is the case $p=2$ of Proposition 4, in view of the relation $\phi_{2^h}(X)=X^{2^{h-1}}+1$. The second relation is the special case $h=1$ of the first one. □

Proposition 5. *The Mersenne numbers are, for prime numbers p,*

$$M_p=2^p-1=N_p\big(\lambda_p^2-1\big)=N_p(1+\lambda_p)=N_p(2-\zeta_p).$$

The Fermat numbers are, for $k\in\mathbb{N}$,

$$F_k=2^{2^k}+1=N_{2^{k+1}}\big(\lambda_{2^{k+1}}^2-1\big)=N_{2^{k+1}}(1+\lambda_{2^{k+1}})=N_{2^{k+1}}(2-\zeta_{2^{k+1}}).$$

Proof. The expression for the Mersenne numbers results from Corollary 2 to Proposition 2, with $q=2$, noting that $\lambda_2=2$ and $N_p(\lambda_p-1)=N_p(-\zeta_p)=1$ by (3).

Similarly, the expression for the Fermat numbers results from the corollary to Proposition 1, with $p=2$. □

Remark 4. The relations $N_p(2-\zeta_p)=\phi_p(2)=2^p-1=M_p$, for a prime p, and $N_{2^{k+1}}(2-\zeta_{2^{k+1}})=\phi_{2^{k+1}}(2)=2^{2^k}+1=F_k$, for $k\in\mathbb{N}$, also follow from (1) in Remark 2.

3. Congruences and prime factors for the norms

Proposition 6. *For any prime number p and any positive integers h, n,*

$$N_{p^h}\big(1-\lambda_{p^h}^n\big)\equiv 1 \pmod{p^{\lceil \frac{n}{\varphi(p^h)}\rceil}},$$

where $\lceil x\rceil$, for a real number x, is the smallest integer $\geqslant x$.

Proof. The rational prime p is totally ramified in the cyclotomic extension $K_{p^h}|\mathbb{Q}$, the only prime ideal of O_{p^h} above p being $(\lambda_{p^h})=\lambda_{p^h}O_{p^h}$, with ramification index $\varphi(p^h)$. So $\sigma((\lambda_{p^h}))=(\lambda_{p^h})$, for any σ in the Galois group G_{p^h} of $K_{p^h}|\mathbb{Q}$. Hence

$$N_{p^h}\big(1-\lambda_{p^h}^n\big)=\prod_{\sigma\in G_{p^h}}\big(1-\sigma(\lambda_{p^h})^n\big)\equiv 1 \pmod{\lambda_{p^h}^n}.$$

In terms of the λ_{p^h}-adic valuation $v_{\lambda_{p^h}}$ of K_{p^h} and of the p-adic valuation v_p of $\mathbb{Q}$, where $N_{p^h}(1-\lambda_{p^h}^n)$ lies, this amounts to $v_{\lambda_{p^h}}(N_{p^h}(1-\lambda_{p^h}^n)-1)=\varphi(p^h)v_p(N_{p^h}(1-\lambda_{p^h}^n)-1)\geqslant n$. The result follows, since $v_p(N_{p^h}(1-\lambda_{p^h}^n)-1)$ is a rational integer. □

Corollary. *For any prime numbers p, q and any positive integers h, k, we have*

$$N_{p^h}\big(\phi_{q^k}(\lambda_{p^h})\big) \equiv 1 \pmod{p^{\lceil \frac{q^k-1}{\varphi(p^h)} \rceil}}.$$

Thus, if $p \neq q$, then

$$N_{p^h}\big(\phi_{q^k}(\lambda_{p^h})\big) = N_{q^k}\big(\phi_{p^h}(\lambda_{q^k})\big) \equiv 1 \pmod{p^{\lceil \frac{q^k-1}{\varphi(p^h)} \rceil} q^{\lceil \frac{p^h-1}{\varphi(q^k)} \rceil}}.$$

In particular, if p and q are distinct odd prime numbers, then

$$N_p\big(1-\lambda_p^q\big) = N_q\big(1-\lambda_q^p\big) \equiv 1 \pmod{p^{\lceil \frac{q}{p-1} \rceil} q^{\lceil \frac{p}{q-1} \rceil}}.$$

Proof. We have $N_{p^h}(\phi_{q^k}(\lambda_{p^h})) = \frac{N_{p^h}(1-\lambda_{p^h}^{q^k})}{N_{p^h}(1-\lambda_{p^h}^{q^{k-1}})}$, where, by Proposition 6, $N_{p^h}(1-\lambda_{p^h}^{q^k}) \equiv 1 \pmod{p^{\lceil \frac{q^k}{\varphi(p^h)} \rceil}}$ and $N_{p^h}(1-\lambda_{p^h}^{q^{k-1}}) \equiv 1 \pmod{p^{\lceil \frac{q^{k-1}}{\varphi(p^h)} \rceil}}$. Therefore $N_{p^h}(1-\lambda_{p^h}^{q^k}) \equiv N_{p^h}(1-\lambda_{p^h}^{q^{k-1}}) \equiv 1 \pmod{p^{\lceil \frac{q^{k-1}}{\varphi(p^h)} \rceil}}$. Since these norms are relatively prime to p, the congruence can be divided by one of them, which yields the first stated congruence.

The second congruence follows from the first one, in view of the corollary to Theorem 1, and taking into account that the difference between each norm and 1 being divisible by prime powers of distinct primes is divisible by their product.

The third congruence follows from Proposition 6, in view of Corollary 2 to Proposition 2, since p and q being odd primes, $N_p(1-\lambda_p^q) = N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1) = N_q(1-\lambda_q^p)$. □

Lemma 2. *Let n be a positive integer and $x \in O_n$. For any prime number l which divides $N_n(x)$, there exists a prime ideal $\mathfrak{l}$ of O_n dividing l and x.*

Proof. The ideal lO_n is a product of prime ideals of O_n which are pairwise conjugates under the action of the Galois group G_n of $K_n|\mathbb{Q}$. Let $\mathfrak{l}_0$ be one of these prime ideals of O_n dividing l. Then $\mathfrak{l}_0$ divides $N_n(x) = \prod_{\sigma \in G_n} \sigma(x)$, and therefore $\mathfrak{l}_0$ divides one of the factors $\sigma(x)$ of the latter product. Then $\mathfrak{l} = \sigma^{-1}(\mathfrak{l}_0)$ is a prime ideal of O_n dividing both l and x. □

Theorem 2. *Let m, n be two positive integers, $x \in O_m$, and l a prime number dividing $N_m(\phi_n(x))$ and relatively prime to mn. Let f_m (resp. f_n) be the order of l modulo m (resp. n). Then f_n divides f_m.*

Proof. By Lemma 2, there exists a prime ideal $\mathfrak{l}$ of O_m dividing l and $\phi_n(x)$. Then $x^n \equiv 1 \pmod{\mathfrak{l}}$, since $\phi_n(x)$ divides $x^n - 1$. So the order h of x modulo $\mathfrak{l}$ divides n. We next prove that $h = n$.

Assume that $h < n$. Then $\mathfrak{l}$ divides $x^h - 1 = \prod_{d|h} \phi_d(x)$. So there exists a positive integer d dividing h such that $\mathfrak{l}$ divides $\phi_d(x)$. Thus $\mathfrak{l}$ divides both $\phi_n(x)$ and $\phi_d(x)$, where $d \mid n$. This means that the canonical images $\overline{\phi_n}$ and $\overline{\phi_d}$ of the polynomials ϕ_n and ϕ_d in $\mathbb{F}_l[X]$ have a common root $\bar{x} = x + \mathfrak{l}$ in the field extension $O_m/\mathfrak{l}$ of $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$. Therefore the resultant $R(\overline{\phi_n}, \overline{\phi_d}) = 0$ in $\mathbb{F}_l$, i.e. l divides the resultant $R(\phi_n, \phi_d)$ in $\mathbb{Z}$ (for the properties of the resultant, see [L]). On the other hand, since ϕ_d divides $X^d - 1$ in $\mathbb{Z}[X]$, by the distributivity property of the resultant, $R(\phi_n, \phi_d)$ divides $R(\phi_n, X^d - 1)$ in $\mathbb{Z}$. Let $n = ad$, where a is a positive integer. Then $\zeta_n^d = \zeta_a$, and

$$R\big(\phi_n, X^d - 1\big) = \prod_{k \in R_n^*} \big(\zeta_n^{kd} - 1\big) = \prod_{k \in R_n^*} \big(\zeta_a^k - 1\big) = N_n(\zeta_a - 1) = (-1)^{\varphi(n)} N_n(1 - \zeta_a).$$

If a has two distinct prime factors, then $1-\zeta_a$ is a unit [W] and therefore $N_n(1-\zeta_a)=\pm 1$. If $a=p^k$ is a power of a prime p dividing n, then $N_n(1-\zeta_a)=N_{K_n|K_{p^k}}(N_{p^k}(1-\zeta_{p^k}))=N_{K_n|K_{p^k}}(p)=p^{[K_n:K_{p^k}]}$ divides a power of n, which, by assumption, is relatively prime to l. In either case, l does not divide $R(\phi_n, X^d-1)$, and therefore l does not divide $R(\phi_n,\phi_d)$, a contradiction. So the assumption $h<n$ cannot hold, and since $h \mid n$, this implies that $h=n$.

The order n of the canonical image of x in the multiplicative group $(O_m/\mathfrak{l})^*$ divides the order $N\mathfrak{l}-1$ of this group, where $N\mathfrak{l}=l^{f_m}$ is the absolute norm of $\mathfrak{l}$. Hence $l^{f_m}\equiv 1 \pmod n$, i.e. f_n divides f_m. □

Theorem 2 has some consequences, which are essential for the sequel, in particular, Corollaries 2 and 4 below.

Corollary 1. *For any positive integer n and any $x\in\mathbb{Z}$, if a prime number l divides $\phi_n(x)$ and does not divide n, then $l\equiv 1 \pmod n$.*

Proof. This follows from Theorem 2 with $m=1$, which implies, for a prime l dividing $\phi_n(x)=N_1(\phi_n(x))$ but not dividing n, that f_n divides $f_1=1$, i.e. $f_n=1$, i.e. $l\equiv 1 \pmod n$. □

Corollary 2. *For any positive integers m, n and any $c\in\mathbb{Z}$, if a prime number l divides $N_m(\phi_n(c-\zeta_m))$ and does not divide mn, then the orders f_m and f_n of l modulo m and modulo n, respectively, are equal.*

In particular, if a prime number l divides $N_m(\phi_n(\lambda_m))$ and does not divide mn, then $f_m=f_n$.

Proof. By Theorem 1, $N_m(\phi_n(c-\zeta_m))=N_n(\phi_m(c-\zeta_n))$ is divisible by l. So, by Theorem 2, f_n divides f_m and f_m divides f_n. Hence $f_m=f_n$. □

Corollary 3. *For any positive integers m, n, if a prime number l divides $N_m(\lambda_m^n-1)$ and does not divide mn, then the order f_m of l modulo m divides the order f_n of l modulo n.*

Proof. We have $\lambda_m^n-1=\prod_{d|n}\phi_d(\lambda_m)$, so that the prime number l divides

$$N_m\big(\lambda_m^n-1\big)=\prod_{d|n}N_m\big(\phi_d(\lambda_m)\big),$$

and therefore l divides $N_m(\phi_d(\lambda_m))$ for some positive divisor d of n, while $l\nmid md$ since $l\nmid mn$. So, by the previous corollary, $f_m=f_d$, and since $d\mid n$, we have $f_d\mid f_n$. Hence $f_m\mid f_n$. □

Corollary 4. *For any positive integer m and any prime number p, if a prime number l divides $N_m(\lambda_m^p-1)$ and does not divide m, then $l\neq p$, and the orders f_m and f_p of l modulo m and modulo p, respectively, are equal.*

In particular, for any prime numbers p,q,l such that l divides $N_p(\lambda_p^q-1)=N_q(\lambda_q^p-1)$, the order f_p of l modulo p is equal to the order f_q of l modulo q.

Proof. Note first that $m\geqslant 2$, since if $m=1$, then $N_1(\lambda_1^p-1)=-1$ has no prime divisor l. By Proposition 2, $N_m(\lambda_m^p-1)=N_m(\phi_p(\lambda_m))=N_p(\phi_m(\lambda_p))$. Since $\phi_m(\lambda_p)$ divides λ_p^m-1 in O_m, the norm $N_p(\phi_m(\lambda_p))$ divides $N_p(\lambda_p^m-1)$ in $\mathbb{Z}$, and by Proposition 6, $N_p(1-\lambda_p^m)\equiv 1 \pmod p$, so that p does not divide $N_p(\lambda_p^m-1)$, and therefore p does not divide $N_p(\phi_m(\lambda_p))=N_m(\lambda_m^p-1)$. Hence $l\neq p$. Then, by Corollary 2 above, $f_m=f_p$.

In the special case where $m=q$ is prime, the equality $N_p(\lambda_p^q-1)=N_q(\lambda_q^p-1)$ is from Corollary 2 to Proposition 2, and, by Proposition 6, a prime divisor l of $N_p(\lambda_p^q-1)=N_q(\lambda_q^p-1)$ is different from p and q. So the result follows from the general case above. □

Theorem 3. *Let n be a positive integer and $c \in \mathbb{Z}$ such that $\gcd(n, \phi_n(c)) = 1$. Then $\phi_n(c)$ is a rational prime if and only if $c - \zeta_n$ is a prime element in the ring of integers O_n of K_n. Moreover, when $\phi_n(c)$ is prime in $\mathbb{Z}$, it splits completely in $K_n|\mathbb{Q}$.*

Proof. Let $(c - \zeta_n)O_n = \prod_{i=1}^{r} \mathfrak{p}_i^{k_i}$ be the prime ideal factorization of $(c - \zeta_n)$ in O_n, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct prime ideals of O_n and $k_1, \ldots, k_r$ are positive integers. By (1) in Remark 2, $\phi_n(c) = N_n(c - \zeta_n)$. For an ideal $\mathfrak{a}$ of O_n, denote by $N\mathfrak{a}$ the absolute norm of $\mathfrak{a}$, i.e. the cardinality $\#(O_n/\mathfrak{a})$ of the corresponding quotient ring. We then have $N\mathfrak{p}_i = p_i^{f_i}$, where p_i is the rational prime below $\mathfrak{p}_i$ and f_i is the residue degree of $\mathfrak{p}_i$ in $K_n|\mathbb{Q}$, for $1 \leqslant i \leqslant r$. Therefore

$$\left|\phi_n(c)\right| = \left|N_n(c - \zeta_n)\right| = \prod_{i=1}^{r} N\mathfrak{p}_i^{k_i} = \prod_{i=1}^{r} p_i^{f_i k_i}.$$

If $|\phi_n(c)|$ is a prime number, then $r = f_1 = k_1 = 1$, and $(c - \zeta_n)O_n = \mathfrak{p}_1$ is a prime ideal of O_n.

Conversely, if $(c - \zeta_n)O_n = \mathfrak{p}$ is a prime ideal of O_n lying above a rational prime p and having residue degree f, then $|\phi_n(c)| = |N_n(c - \zeta_n)| = N\mathfrak{p} = p^f$. So p divides $\phi_n(c)$, and, since n and $\phi_n(c)$ are relatively prime, p does not divide n. Therefore $p \equiv 1 \pmod{n}$, by Corollary 1 to Theorem 2. Hence p splits completely in $K_n|\mathbb{Q}$, i.e. $f = 1$ and $|\phi_n(c)| = p$ is a product of $\varphi(n) = [K_n : \mathbb{Q}]$ distinct prime ideals of O_n, the Galois conjugates of $\mathfrak{p}$ [W]. Thus $|\phi_n(c)|$ is a prime number p which splits completely in $K_n|\mathbb{Q}$. □

Remark 5. The assumption $\gcd(n, \phi_n(c)) = 1$ is not necessary to establish that if $|\phi_n(c)|$ is a prime number, then $c - \zeta_n$ is a prime element in O_n, as seen from the first part of the proof of Theorem 3. It is only needed in the proof of the converse.

If $n \geqslant 3$, then $N_n(x) \geqslant 0$ for all $x \in K_n$ (since the product of the Galois conjugates of x can be written as a product of pairs of complex conjugates), so that $|\phi_n(c)|$ can be replaced by $\phi_n(c)$ in that case.

Corollary. *For any prime number p, any $k \in \mathbb{N}$, and any $c \in \mathbb{Z}$ such that $c \not\equiv 1 \pmod{p}$, the rational integer $N_{p^{k+1}}(c - \zeta_{p^{k+1}}) = \phi_{p^{k+1}}(c) = \sum_{j=0}^{p-1} c^{p^k j}$ is a rational prime if and only if the cyclotomic integer $c - \zeta_{p^{k+1}}$ is a prime element in the ring of integers $O_{p^{k+1}}$ of $K_{p^{k+1}}$. And when this is the case, the rational prime splits completely in $K_{p^{k+1}}|\mathbb{Q}$.*

In particular, for any prime number p, the Mersenne number $M_p = 2^p - 1 = \phi_p(2) = N_p(2 - \zeta_p)$ is a prime number if and only if $2 - \zeta_p$ is a prime element in the ring of integers O_p of K_p. Moreover, when M_p is prime, it splits completely in $K_p|\mathbb{Q}$.

Similarly, for any $k \in \mathbb{N}$, the Fermat number $F_k = 2^{2^k} + 1 = \phi_{2^{k+1}}(2) = N_{2^{k+1}}(2 - \zeta_{2^{k+1}})$ is a prime number if and only if $2 - \zeta_{2^{k+1}}$ is a prime element in the ring of integers $O_{2^{k+1}}$ of $K_{2^{k+1}}$. Moreover, when F_k is prime, it splits completely in $K_{2^{k+1}}|\mathbb{Q}$.

Proof. The first statement follows from Theorem 3 with $n = p^{k+1}$. The condition $c \not\equiv 1 \pmod{p}$ implies that $c^{p^{k+1}} \equiv c^{p^k} \equiv \cdots \equiv c^p \equiv c \not\equiv 1 \pmod{p}$, and therefore $\phi_{p^{k+1}}(c) \not\equiv 0 \pmod{p}$, since $\phi_{p^{k+1}}(c)$ divides $c^{p^{k+1}} - 1$, which secures the condition $\gcd(p^{k+1}, \phi_{p^{k+1}}(c)) = 1$.

The second and third statements are respectively the special cases $k = 0$, $c = 2$ and $p = 2$, $c = 2$ of the first one. □

4. Properties of the prime ideal factors of certain cyclotomic integers

Notations. For a positive integer n, we denote by $\mathbb{P}(O_n)$ the set of prime ideals of the ring of integers O_n of K_n, and for $\mathfrak{l} \in \mathbb{P}(O_n)$, we denote by $v_{\mathfrak{l}}$ the $\mathfrak{l}$-adic valuation of K_n.

Proposition 7. *Let m, n be two positive integers, $c \in \mathbb{Z}$, and l a prime number dividing $N_m(\phi_n(c-\zeta_m)) = N_n(\phi_m(c-\zeta_n))$ and relatively prime to mn. Then*

$$\sum_{\substack{\mathfrak{l}\in\mathbb{P}(O_m)\\ \mathfrak{l}\mid l}} v_{\mathfrak{l}}\big(\phi_n(c-\zeta_m)\big) = \sum_{\substack{\mathfrak{l}'\in\mathbb{P}(O_n)\\ \mathfrak{l}'\mid l}} v_{\mathfrak{l}'}\big(\phi_m(c-\zeta_n)\big).$$

Proof. The equality $N_m(\phi_n(c-\zeta_m)) = N_n(\phi_m(c-\zeta_n))$ follows from Theorem 1.

Since $l \nmid mn$, the prime l is unramified in $K_m|\mathbb{Q}$ and in $K_n|\mathbb{Q}$. So, for any $\mathfrak{l} \in \mathbb{P}(O_m)$ such that $\mathfrak{l} \mid l$,

$$v_l\big(N_m\big(\phi_n(c-\zeta_m)\big)\big) = v_{\mathfrak{l}}\big(N_m\big(\phi_n(c-\zeta_m)\big)\big) = v_{\mathfrak{l}}\Big(\prod_{\sigma\in G_m}\sigma\big(\phi_n(c-\zeta_m)\big)\Big)$$
$$= \sum_{\sigma\in G_m} v_{\mathfrak{l}}\big(\sigma\big(\phi_n(c-\zeta_m)\big)\big).$$

Let f_m be the order of l modulo m. Then f_m is the residue class degree of $\mathfrak{l}$ over l, and the sequence of conjugates $\sigma(\mathfrak{l})$ of $\mathfrak{l}$, for $\sigma \in G_m = Gal(K_m|\mathbb{Q})$, consists of all the distinct prime ideals of O_m which divide l, each one repeated f_m times [W]. Moreover, $v_{\mathfrak{l}}(\sigma(x)) = v_{\sigma^{-1}(\mathfrak{l})}(x)$, for any $x \in K_m$. Therefore

$$\sum_{\sigma\in G_m} v_{\mathfrak{l}}\big(\sigma\big(\phi_n(c-\zeta_m)\big)\big) = \sum_{\sigma\in G_m} v_{\sigma^{-1}(\mathfrak{l})}\big(\phi_n(c-\zeta_m)\big) = f_m \sum_{\substack{\mathfrak{l}\in\mathbb{P}(O_m)\\ \mathfrak{l}\mid l}} v_{\mathfrak{l}}\big(\phi_n(c-\zeta_m)\big).$$

Thus

$$v_l\big(N_m\big(\phi_n(c-\zeta_m)\big)\big) = f_m \sum_{\substack{\mathfrak{l}\in\mathbb{P}(O_m)\\ \mathfrak{l}\mid l}} v_{\mathfrak{l}}\big(\phi_n(c-\zeta_m)\big). \tag{5}$$

Similarly, exchanging m and n, we get

$$v_l\big(N_n\big(\phi_m(c-\zeta_n)\big)\big) = f_n \sum_{\substack{\mathfrak{l}'\in\mathbb{P}(O_n)\\ \mathfrak{l}'\mid l}} v_{\mathfrak{l}'}\big(\phi_m(c-\zeta_n)\big),$$

where f_n is the order of l modulo n. Since $N_m(\phi_n(c-\zeta_m)) = N_n(\phi_m(c-\zeta_n))$, then

$$f_m \sum_{\substack{\mathfrak{l}\in\mathbb{P}(O_m)\\ \mathfrak{l}\mid l}} v_{\mathfrak{l}}\big(\phi_n(c-\zeta_m)\big) = f_n \sum_{\substack{\mathfrak{l}'\in\mathbb{P}(O_n)\\ \mathfrak{l}'\mid l}} v_{\mathfrak{l}'}\big(\phi_m(c-\zeta_n)\big).$$

And, by Corollary 2 to Theorem 2, $f_m = f_n$. The result follows. □

Corollary 1. *For any prime numbers p, q, l such that l divides $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$,*

$$\sum_{\substack{\mathfrak{l}\in\mathbb{P}(O_p)\\ \mathfrak{l}\mid l}} v_{\mathfrak{l}}\big(1-\lambda_p^q\big) = \sum_{\substack{\mathfrak{l}'\in\mathbb{P}(O_q)\\ \mathfrak{l}'\mid l}} v_{\mathfrak{l}'}\big(1-\lambda_q^p\big) = \frac{1}{f} v_l\big(N_p\big(\lambda_p^q - 1\big)\big),$$

where f is the common order of l modulo p and modulo q.

Proof. By Proposition 2, $N_q(\lambda_q^p - 1) = N_q(\phi_p(\lambda_q)) = N_p(\phi_q(\lambda_p)) = N_p(\lambda_p^q - 1)$, and by Proposition 6, p and q do not divide $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$, i.e. $l \neq p, q$. Then, by Proposition 7,

$$\sum_{\substack{\mathfrak{l} \in \mathbb{P}(O_p) \\ \mathfrak{l} | l}} v_{\mathfrak{l}}\big(\phi_q(\lambda_p)\big) = \sum_{\substack{\mathfrak{l}' \in \mathbb{P}(O_q) \\ \mathfrak{l}' | l}} v_{\mathfrak{l}'}\big(\phi_p(\lambda_q)\big).$$

Moreover, $\phi_q(\lambda_p) = \frac{1-\lambda_p^q}{1-\lambda_p} = \frac{1-\lambda_p^q}{\zeta_p}$, so that $v_{\mathfrak{l}}(\phi_q(\lambda_p)) = v_{\mathfrak{l}}(1 - \lambda_p^q)$, for any $\mathfrak{l} \in \mathbb{P}(O_p)$, and a similar relation holds with p and q exchanged. The result follows, in view of (5). □

Corollary 2. *Let m, n be two positive integers and $c \in \mathbb{Z}$ such that $N_m(\phi_n(c - \zeta_m))$ is relatively prime to mn. Let $|N_m(\phi_n(c - \zeta_m))| = |N_n(\phi_m(c - \zeta_n))| = \prod_{i=1}^r l_i^{h_i}$, with distinct prime numbers $l_1, \ldots, l_r$ and positive integers $h_1, \ldots, h_r$, be the prime factorization of the norm. For $1 \leqslant i \leqslant r$, let f_i be the order of l_i modulo m and modulo n. Then f_i divides h_i for all $1 \leqslant i \leqslant r$.*

In particular, for any prime numbers p, q, if $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1) = \prod_{i=1}^r l_i^{h_i}$, where $l_1, \ldots, l_r$ are distinct prime numbers and $h_1, \ldots, h_r$ are positive integers, then every h_i is divisible by the order f_i of l_i modulo p and modulo q, for $1 \leqslant i \leqslant r$.

Proof. The first part follows from formula (5) in the proof of Proposition 7, which gives for every $1 \leqslant i \leqslant r$,

$$h_i = v_{l_i}\big(N_m\big(\phi_n(c - \zeta_m)\big)\big) = f_i \sum_{\substack{\mathfrak{l}_i \in \mathbb{P}(O_m) \\ \mathfrak{l}_i | l_i}} v_{\mathfrak{l}_i}\big(\phi_n(c - \zeta_m)\big).$$

The second part follows from the first one, since, by Proposition 2, $N_p(\lambda_p^q - 1) = N_p(\phi_q(1 - \zeta_p)) = N_q(\phi_p(1 - \zeta_q)) = N_q(\lambda_q^p - 1)$, and by Proposition 6, all $l_i \neq p, q$, so that $N_p(\phi_q(1 - \zeta_p))$ is relatively prime to pq. □

Theorem 4. *Let m, n be two positive integers and $c \in \mathbb{Z}$ such that $N_m(\phi_n(c - \zeta_m))$ is relatively prime to mn. Let $|N_m(\phi_n(c - \zeta_m))| = |N_n(\phi_m(c - \zeta_n))| = \prod_{i=1}^r l_i^{h_i}$, where $l_1, \ldots, l_r$ are distinct prime numbers and $h_1, \ldots, h_r$ are positive integers. For $1 \leqslant i \leqslant r$, let f_i be the order of l_i modulo m and modulo n and $m_i = \frac{h_i}{f_i}$, and let $\mathfrak{l}_i$ (resp. $\mathfrak{l}_i'$) be a prime ideal of O_m (resp. O_n) dividing l_i and $\phi_n(c - \zeta_m)$ (resp. dividing l_i and $\phi_m(c - \zeta_n)$). Then*

$$\phi_n(c - \zeta_m) O_m = \prod_{i=1}^r \mathfrak{l}_{i,1} \ldots \mathfrak{l}_{i,m_i},$$

and

$$\phi_m(c - \zeta_n) O_n = \prod_{i=1}^r \mathfrak{l}'_{i,1} \ldots \mathfrak{l}'_{i,m_i},$$

where $\mathfrak{l}_{i,1}, \ldots, \mathfrak{l}_{i,m_i}$ (resp. $\mathfrak{l}'_{i,1}, \ldots, \mathfrak{l}'_{i,m_i}$) are m_i, not necessarily distinct, prime ideal conjugates of $\mathfrak{l}_i$ in O_m (resp. of $\mathfrak{l}_i'$ in O_n), for every $1 \leqslant i \leqslant r$.

Proof. Note that in the statement, we implicitly use Theorem 1 for the equality of the norms, Corollary 2 to Theorem 2 for the equality of the orders of l_i modulo m and modulo n, Corollary 2 to Proposition 7 for the divisibility of h_i by f_i thus yielding an integral quotient m_i, and Lemma 2 for the existence of the prime ideal $\mathfrak{l}_i$ (resp. $\mathfrak{l}_i'$), for each i.

Since $N_m(\phi_n(c-\zeta_m))$ is relatively prime to mn, all the prime numbers l_i are unramified in $K_m|\mathbb{Q}$ and in $K_n|\mathbb{Q}$. For $1 \leqslant i \leqslant r$, we then have the prime ideal factorization $l_i O_m = \prod_{s=1}^{g_i} \mathfrak{l}_{i,s}^*$, where $\mathfrak{l}_{i,1}^*, \ldots, \mathfrak{l}_{i,g_i}^*$ are distinct prime ideals of O_m, conjugates of $\mathfrak{l}_i$, each of residue degree f_i and absolute norm $N\mathfrak{l}_{i,s}^* = l_i^{f_i}$, with $g_i = \frac{\varphi(m)}{f_i}$ [W]. Since $\phi_n(c-\zeta_m)$ divides $|N_m(\phi_n(c-\zeta_m))| = \prod_{i=1}^r l_i^{h_i}$ in O_m, and the integers $l_i^{h_i}$ are pairwise relatively prime, $\phi_n(c-\zeta_m)O_m = \prod_{i=1}^r \gcd(\phi_n(c-\zeta_m)O_m, l_i^{h_i} O_m)$, and $\gcd(\phi_n(c-\zeta_m)O_m, l_i^{h_i} O_m) = \gcd(\phi_n(c-\zeta_m)O_m, \prod_{s=1}^{g_i} \mathfrak{l}_{i,s}^{*\,h_i}) = \prod_{s=1}^{g_i} \mathfrak{l}_{i,s}^{*\,a_{i,s}}$, where each $a_{i,s}$ is an integer $\geqslant 0$, equal to the $\mathfrak{l}_{i,s}^*$-adic valuation of $\phi_n(c-\zeta_m)$, for $1 \leqslant s \leqslant g_i$ and $1 \leqslant i \leqslant r$. Therefore

$$\phi_n(c-\zeta_m)O_m = \prod_{i=1}^{r} \prod_{s=1}^{g_i} \mathfrak{l}_{i,s}^{*\,a_{i,s}}.$$

Moreover,

$$\prod_{i=1}^{r} l_i^{h_i} = \left|N_m\big(\phi_n(c-\zeta_m)\big)\right| = \prod_{i=1}^{r} \prod_{s=1}^{g_i} N\mathfrak{l}_{i,s}^{*\,a_{i,s}} = \prod_{i=1}^{r} \prod_{s=1}^{g_i} l_i^{f_i a_{i,s}} = \prod_{i=1}^{r} l_i^{\sum_{s=1}^{g_i} f_i a_{i,s}}.$$

Hence $\sum_{s=1}^{g_i} f_i a_{i,s} = h_i$, i.e. $\sum_{s=1}^{g_i} a_{i,s} = m_i$, i.e. $\gcd(\phi_n(c-\zeta_m)O_m, l_i^{h_i} O_m) = \prod_{s=1}^{g_i} \mathfrak{l}_{i,s}^{*\,a_{i,s}}$ is the product of m_i, not necessarily distinct, prime ideals of O_m, all conjugates of $\mathfrak{l}_i$, for $1 \leqslant i \leqslant r$. Thus $\prod_{s=1}^{g_i} \mathfrak{l}_{i,s}^{*\,a_{i,s}} = \mathfrak{l}_{i,1} \ldots \mathfrak{l}_{i,m_i}$, for $1 \leqslant i \leqslant r$, and

$$\phi_n(c-\zeta_m)O_m = \prod_{i=1}^{r} \mathfrak{l}_{i,1} \ldots \mathfrak{l}_{i,m_i},$$

where $\mathfrak{l}_{i,1}, \ldots, \mathfrak{l}_{i,m_i}$ are m_i, not necessarily distinct, prime ideals of O_m, all conjugates of $\mathfrak{l}_i$, for every $1 \leqslant i \leqslant r$.

Similar relations hold in $K_n|\mathbb{Q}$, with m and n exchanged, giving the prime ideal factorization $\phi_m(c-\zeta_n)O_n = \prod_{i=1}^r \prod_{t=1}^{g_i'} \mathfrak{l}_{i,t}'^{*\,b_{i,t}}$, where, for every i, $g_i' = \frac{\varphi(n)}{f_i}$, and $\mathfrak{l}_{i,t}'^*$, for $1 \leqslant t \leqslant g_i'$, are the distinct prime ideals of O_n above l_i, conjugates of $\mathfrak{l}_i'$, each of residue degree f_i in $K_n|\mathbb{Q}$ (the same as that of $\mathfrak{l}_i$ in $K_m|\mathbb{Q}$), and the $b_{i,t}$ are integers $\geqslant 0$. Moreover, since $\prod_{i=1}^r l_i^{h_i} = |N_n(\phi_m(c-\zeta_n))| = \prod_{i=1}^r \prod_{t=1}^{g_i'} N\mathfrak{l}_{i,t}'^{*\,b_{i,t}} = \prod_{i=1}^r \prod_{t=1}^{g_i'} l_i^{f_i b_{i,t}}$, for every $1 \leqslant i \leqslant r$, we similarly have $\sum_{t=1}^{g_i'} b_{i,t} = m_i$, so that $\prod_{t=1}^{g_i'} \mathfrak{l}_{i,t}'^{*\,b_{i,t}}$ is the product of m_i, not necessarily distinct, prime ideals $\mathfrak{l}_{i,1}', \ldots, \mathfrak{l}_{i,m_i}'$ of O_n, conjugates of $\mathfrak{l}_i'$. Thus

$$\phi_m(c-\zeta_n)O_n = \prod_{i=1}^{r} \mathfrak{l}_{i,1}' \ldots \mathfrak{l}_{i,m_i}'. \qquad \square$$

Remark 6. Given the rational prime factorization $|N_m(\phi_n(c-\zeta_m))| = |N_n(\phi_m(c-\zeta_n))| = \prod_{i=1}^r l_i^{h_i}$, Theorem 4 shows that there is a symmetry between the prime ideal factorization of $\phi_n(c-\zeta_m)O_m$ in O_m and that of $\phi_m(c-\zeta_n)O_n$ in O_n. Indeed, these two principal ideals are each a product, for i ranging from 1 to r, of products of m_i (not necessarily distinct) prime ideals lying above l_i.

Corollary. *Keeping the notations and assumptions of Theorem 4, if* $|N_m(\phi_n(c-\zeta_m))| = |N_n(\phi_m(c-\zeta_n))| = \prod_{i=1}^r l_i^{f_i}$, *where* f_i *is the order of the prime number* l_i *modulo* m *and modulo* n $(1 \leqslant i \leqslant r)$, *then*

$$\phi_n(c-\zeta_m)O_m = \prod_{i=1}^{r} \mathfrak{l}_i, \qquad \phi_m(c-\zeta_n)O_n = \prod_{i=1}^{r} \mathfrak{l}'_i,$$

where, for every i, $\mathfrak{l}_i$ (resp. $\mathfrak{l}'_i$) is the unique prime ideal of O_m (resp. of O_n) dividing l_i and $\phi_n(c-\zeta_m)$ (resp. dividing l_i and $\phi_m(c-\zeta_n)$).

Proof. This is the special case of Theorem 4 where, for every $1 \leqslant i \leqslant r$, we have $m_i = 1$, so that, from the proof of Theorem 4, $\gcd(\phi_n(c-\zeta_m)O_m, l_i^{h_i} O_m) = \mathfrak{l}_i$, hence the uniqueness of the prime ideal $\mathfrak{l}_i$ of O_m dividing l_i and $\phi_n(c-\zeta_m)$, and the prime ideal factorization $\phi_n(c-\zeta_m)O_m = \prod_{i=1}^{r} \mathfrak{l}_i$. By symmetry, exchanging m and n, we get similar results for $\phi_m(c-\zeta_n)O_n$. □

Theorem 5. *Let m, n be two positive integers and $c \in \mathbb{Z}$ such that $N_m(\phi_n(c-\zeta_m))$ is relatively prime to mn. The following three conditions are equivalent*:

(1) *$\phi_n(c-\zeta_m)O_m$ is a prime ideal of O_m;*
(2) *$|N_m(\phi_n(c-\zeta_m))| = |N_n(\phi_m(c-\zeta_n))| = l^f$, where l is a prime number whose order modulo m and modulo n is f;*
(3) *$\phi_m(c-\zeta_n)O_n$ is a prime ideal of O_n.*

Proof. By Theorem 4, to the rational prime factorization $|N_m(\phi_n(c-\zeta_m))| = |N_n(\phi_m(c-\zeta_n))| = \prod_{i=1}^{r} l_i^{h_i}$ corresponds the prime ideal factorization $\phi_n(c-\zeta_m)O_m = \prod_{i=1}^{r} \mathfrak{l}_{i,1} \dots \mathfrak{l}_{i,m_i}$, where $\mathfrak{l}_{i,1}, \dots, \mathfrak{l}_{i,m_i}$ are $m_i = \frac{h_i}{f_i}$, not necessarily distinct, prime ideals of O_m above l_i, and f_i is the order of l_i modulo m and modulo n, for every $1 \leqslant i \leqslant r$. Therefore $\phi_n(c-\zeta_m)O_m$ is a prime ideal of O_m if and only if $r = 1$ and $m_1 = \frac{h_1}{f_1} = 1$, i.e. $|N_m(\phi_n(c-\zeta_m))| = |N_n(\phi_m(c-\zeta_n))| = l_1^{f_1}$. Hence the equivalence of the conditions (1) and (2).

Similarly, exchanging m and n, we get the equivalence of conditions (2) and (3). □

Theorem 6. *Let p, q be two prime numbers, and $N_p(\lambda_q^q - 1) = N_q(\lambda_q^p - 1) = \prod_{i=1}^{r} l_i^{h_i}$, where $l_1, \dots, l_r$ are distinct prime numbers and $h_1, \dots, h_r$ are positive integers. For $1 \leqslant i \leqslant r$, let f_i be the order of l_i modulo p and modulo q and $m_i = \frac{h_i}{f_i}$, and let $\mathfrak{l}_i$ (resp. $\mathfrak{l}'_i$) be a prime ideal of O_p (resp. O_q) dividing l_i and $1 - \lambda_p^q$ (resp. dividing l_i and $1 - \lambda_q^p$). Then*

$$\left(1-\lambda_p^q\right)O_p = \prod_{i=1}^{r} \mathfrak{l}_{i,1} \dots \mathfrak{l}_{i,m_i}, \qquad \left(1-\lambda_q^p\right)O_q = \prod_{i=1}^{r} \mathfrak{l}'_{i,1} \dots \mathfrak{l}'_{i,m_i},$$

where, for every i, $\mathfrak{l}_{i,1}, \dots, \mathfrak{l}_{i,m_i}$ (resp. $\mathfrak{l}'_{i,1}, \dots, \mathfrak{l}'_{i,m_i}$) are m_i, not necessarily distinct, prime ideal conjugates of $\mathfrak{l}_i$ in O_p (resp. of $\mathfrak{l}'_i$ in O_q).

In particular, if $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1) = \prod_{i=1}^{r} l_i^{f_i}$, then, for every $1 \leqslant i \leqslant r$, there is a unique prime ideal $\mathfrak{l}_i$ of O_p (resp. $\mathfrak{l}'_i$ of O_q) dividing l_i and $1 - \lambda_p^q$ (resp. dividing l_i and $1 - \lambda_q^p$), and we have

$$\left(1-\lambda_p^q\right)O_p = \prod_{i=1}^{r} \mathfrak{l}_i, \qquad \left(1-\lambda_q^p\right)O_q = \prod_{i=1}^{r} \mathfrak{l}'_i.$$

Furthermore, $1 - \lambda_p^q$ is a prime element in O_p if and only if $1 - \lambda_q^p$ is a prime element in O_q, both primality conditions being equivalent to the equality $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1) = l^f$ with a prime number l whose order modulo p and modulo q is f.

Proof. This follows from Theorem 4 and its corollary and from Theorem 5, since, by Proposition 2, $N_p(\lambda_p^q - 1) = N_p(\phi_q(1-\zeta_p)) = N_q(\phi_p(1-\zeta_q)) = N_q(\lambda_q^p - 1)$, and by Proposition 6, all $l_i \neq p, q$. □

Remark 7. Theorems 5 and 6 establish a reciprocity relation between two cyclotomic fields K_m and K_n (resp. K_p and K_q), namely the primality of an element $\phi_n(c-\zeta_m)$ in O_m (resp. $1-\lambda_p^q$ in O_p) is equivalent to the primality of $\phi_m(c-\zeta_n)$ in O_n (resp. $1-\lambda_q^p$ in O_q).

Proposition 8. *Let p, q and l be prime numbers such that l divides $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$, and let f be the order of l modulo p and modulo q. For any integer n not divisible by p (resp. by q), consider the cyclotomic unit $u_{p,n} = \frac{1-\zeta_p^n}{1-\zeta_p}$ (resp. $u_{q,n} = \frac{1-\zeta_q^n}{1-\zeta_q}$). Then there exists a prime ideal $\mathfrak{l}$ of O_p (resp. $\mathfrak{l}'$ of O_q) dividing l and $1-\lambda_p^q$ and $u_{p,l^i}^q - 1$ (resp. dividing l and $1-\lambda_q^p$ and $u_{q,l^i}^p - 1$) for all $1 \leqslant i \leqslant f$.*

In particular, if $f > 1$, there exists an integer $2 \leqslant j \leqslant p-1$ (resp. $2 \leqslant k \leqslant q-1$) such that $\mathfrak{l}$ divides l and $1-\lambda_p^q$ and $u_{p,j}^q - 1$ (resp. $\mathfrak{l}'$ divides l and $1-\lambda_q^p$ and $u_{q,k}^p - 1$). If, in addition, $p \neq q$, then $2 \leqslant j \leqslant p-2$ (resp. $2 \leqslant k \leqslant q-2$).

Proof. Note that Corollary 2 to Proposition 2 and Corollary 4 to Theorem 2 are implicitly used in the above statement. By Lemma 2, there exists a prime ideal $\mathfrak{l}$ of O_p such that $\mathfrak{l}$ divides l and $1-\lambda_p^q$. The decomposition group of $\mathfrak{l}$ in $K_p|\mathbb{Q}$, consisting of the automorphisms of $K_p|\mathbb{Q}$ which leave $\mathfrak{l}$ fixed, is generated by the Frobenius automorphism $\sigma_l^{(p)}$ and is thus isomorphic to the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ generated by the congruence class of l modulo p, which has order f [W]. So, if an integer $n \equiv l^i \pmod p$, for some $1 \leqslant i \leqslant f$, then $\mathfrak{l} = \sigma_n^{(p)}(\mathfrak{l})$ divides $\sigma_n^{(p)}(1-\lambda_p^q) = 1 - \sigma_n^{(p)}(\lambda_p)^q$. Therefore $\mathfrak{l}$ divides $1-\lambda_p^q - (1-\sigma_n^{(p)}(\lambda_p)^q) = \sigma_n^{(p)}(\lambda_p)^q - \lambda_p^q$. Moreover, $\sigma_n^{(p)}(\lambda_p) = 1-\zeta_p^n = u_{p,n}\lambda_p$, with the cyclotomic unit $u_{p,n} = \frac{1-\zeta_p^n}{1-\zeta_p}$ (this is more generally valid for any integer n not divisible by p). So $\mathfrak{l}$ divides $\sigma_n^{(p)}(\lambda_p)^q - \lambda_p^q = \lambda_p^q(u_{p,n}^q - 1)$, and since λ_p divides p and $\mathfrak{l}$ divides l, with p and l relatively prime (by Proposition 6), then $\mathfrak{l}$ is relatively prime to λ_p, and therefore it divides $u_{p,n}^q - 1$. Thus $\mathfrak{l}$ divides $u_{p,l^i}^q - 1$ for $1 \leqslant i \leqslant f$.

Assume that $f > 1$. Then there exists an integer $1 \leqslant i \leqslant f-1$, so that $l^i \not\equiv 1 \pmod p$, i.e. $l^i \equiv j \pmod p$ for some $2 \leqslant j \leqslant p-1$, and by what precedes, $\mathfrak{l}$ divides $u_{p,l^i}^q - 1 = u_{p,j}^q - 1$. Note that in this case, $p \geqslant 3$, and similarly, by symmetry, $q \geqslant 3$. Further note that $u_{p,p-1} = \frac{1-\zeta_p^{-1}}{1-\zeta_p} = -\zeta_p^{-1}$, and $u_{p,p-1}^q - 1 = -\zeta_p^{-q}(1+\zeta_p^q)$. Thus, if $p \neq q$, then $u_{p,p-1}^q - 1 = -\zeta_p^{-q}\sigma_q^{(p)}(1+\zeta_p) = -\zeta_p^{-q}\sigma_q^{(p)}(u_{p,2})$ is a unit in O_p, not divisible by $\mathfrak{l}$, so that j cannot equal $p-1$, i.e. $2 \leqslant j \leqslant p-2$.

Similar results hold in O_q in view of the symmetry of p and q in the equality $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$ and of the fact that l has the same order modulo p and modulo q. □

Corollary 1. *If one of two distinct prime numbers p, q is equal to 2 or 3, then for any prime number l dividing $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$, we have $l \equiv 1 \pmod{pq}$.*

In other words,

(1) *For any prime numbers $p \neq 2$ and l dividing $N_p(\lambda_p^2 - 1) = 2^p - 1$, we have $l \equiv 1 \pmod{2p}$.*
(2) *For any prime numbers $p \neq 3$ and l dividing $N_p(\lambda_p^3 - 1) = N_3(\lambda_3^p - 1)$, we have $l \equiv 1 \pmod{3p}$.*

Proof. If $p = 2$ (resp. $q = 2$), then there is no integer $2 \leqslant j \leqslant p-1$ (resp. $2 \leqslant k \leqslant q-1$), and therefore, by Proposition 8, the order f of l modulo p and modulo q cannot be > 1. Furthermore, if p and q are odd, with one of them equal to 3, e.g. $q = 3$, then there is no integer $2 \leqslant k \leqslant q-2$, and therefore, by Proposition 8, f cannot be > 1. Thus, in any case, $f = 1$, i.e. $l \equiv 1$ modulo p and modulo q, i.e. $l \equiv 1 \pmod{pq}$. □

Corollary 2. *If p, q are distinct prime numbers, and l is a prime number dividing $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$, then the order f of l modulo p and modulo q is an odd integer.*

Proof. If p or q is equal to 2, then by Corollary 1, $f = 1$ and the result holds trivially. So, we may assume p and q to be distinct odd primes. By Proposition 8, there exists a prime ideal $\mathfrak{l}$ of O_p such that $\mathfrak{l}$ divides l and $1-\lambda_p^q$ and $u_{p,l^i}^q - 1$ for all $1 \leqslant i \leqslant f$. Moreover, by the proof of Proposition 8, $\mathfrak{l}$ does not divide $u_{p,p-1}^q - 1$. Hence $p-1$ is not congruent to a power of l modulo p, i.e. $l^i \not\equiv -1 \pmod{p}$ for any positive integer i. As $p > 2$, this means that the order f of l modulo p is odd. □

Corollary 3. *If p, q are distinct prime numbers such that $\gcd(p-1, q-1)$ is a power of 2, then any prime number l dividing $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$ satisfies $l \equiv 1 \pmod{pq}$.*

In particular, if $p = 2^{2^k} + 1$ is a Fermat prime, then, for any prime numbers $q \neq p$ and l dividing $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$, we have $l \equiv 1 \pmod{pq}$.

Proof. It follows from Corollary 4 to Theorem 2 and from Corollary 2 above that the common order f of l modulo p and modulo q is an odd integer dividing both $p-1$ and $q-1$, and therefore dividing $\gcd(p-1, q-1)$, which is a power of 2. Thus $f = 1$, i.e. $l \equiv 1$ modulo p and modulo q and therefore modulo pq. □

Remark 8. Given prime numbers p, q and l such that l divides $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$, if there exist two distinct prime ideals of O_p dividing l and $1 - \lambda_p^q$, then they are conjugates (as are all the prime ideal factors of l in O_p), of the form $\mathfrak{l}$ and $\sigma_n^{(p)}(\mathfrak{l}) \neq \mathfrak{l}$, for some $2 \leqslant n \leqslant p-1$. Letting j be an inverse of n modulo p, it follows that $\mathfrak{l}$ divides $\sigma_j^{(p)}(1-\lambda_p^q) = 1 - \sigma_j^{(p)}(\lambda_p)^q$, and therefore $\mathfrak{l}$ divides $1-\lambda_p^q-(1-\sigma_j^{(p)}(\lambda_p)^q) = \sigma_j^{(p)}(\lambda_p)^q - \lambda_p^q = \lambda_p^q(u_{p,j}^q - 1)$, where $u_{p,j} = \frac{1-\zeta_p^j}{1-\zeta_p}$ is a cyclotomic unit in O_p. As in the proof of Proposition 8, this means that $\mathfrak{l}$ divides $u_{p,j}^q - 1$ for some $2 \leqslant j \leqslant p-1$, and when p and q are distinct odd primes, j cannot equal $p-1$, so that $2 \leqslant j \leqslant p-2$. However, unlike the case in Proposition 8, since $\sigma_j^{(p)}(\mathfrak{l}) \neq \mathfrak{l}$, the automorphism $\sigma_j^{(p)}$ does not lie in the decomposition group of $\mathfrak{l}$, i.e. j is not congruent to a power of l modulo p.

Corollary. *Let q be a prime number $\geqslant 5$. For any prime number l dividing $N_q(\lambda_q^3 - 1) = N_3(\lambda_3^q - 1)$, there exists a unique prime ideal $\mathfrak{l}$ of O_3 dividing l and $1 - \lambda_3^q$.*

Proof. The existence of $\mathfrak{l}$ results from Lemma 2, and its uniqueness follows from Remark 8, since $q \geqslant 5$ and $p = 3$ are distinct odd primes and there are no integers $2 \leqslant j \leqslant p-2$, so that l and $1 - \lambda_3^q$ cannot have two distinct prime ideal divisors in O_3. □

Lemma 3. *Let m, n be two relatively prime positive integers, and $c \in \mathbb{Z}$. For any prime number l which divides $N_m(\phi_n(c - \zeta_m))$, there exists a prime ideal $\mathfrak{L}$ of O_{mn} dividing l and $c - \zeta_m - \zeta_n$.*

Proof. Since $\gcd(m, n) = 1$, the compositum of K_m and K_n is $K_m K_n = K_{mn}$, whose Galois group over $\mathbb{Q}$ is $G_{mn} \simeq G_m \times G_n$. Thus, by Theorem 1, $N_m(\phi_n(c - \zeta_m)) = N_n(\phi_m(c - \zeta_n)) = N_{mn}(c - \zeta_m - \zeta_n) = \prod_{k \in R_{mn}^*}(c - \zeta_m^k - \zeta_n^k)$.

The ideal lO_{mn} is a product of prime ideals of O_{mn} which are pairwise conjugates under the action of the Galois group G_{mn}. Let $\mathfrak{L}_0$ be one of the prime ideals of O_{mn} dividing l. Then $\mathfrak{L}_0$ divides the product $N_m(\phi_n(c - \zeta_m)) = \prod_{k \in R_{mn}^*}(c - \zeta_m^k - \zeta_n^k)$, and therefore $\mathfrak{L}_0$ divides one of its factors $c - \zeta_m^k - \zeta_n^k$. Hence $\mathfrak{L} = (\sigma_k^{(mn)})^{-1}(\mathfrak{L}_0)$ is a prime ideal of O_{mn} which divides l and $c - \zeta_m - \zeta_n$. □

Remark 9. If, in addition to $\gcd(m, n) = 1$, we also assume that the prime factor l of $N_m(\phi_n(c - \zeta_m))$ is relatively prime to mn, then, using arguments as in the proof of Proposition 7, we get an analogue of formula (5), namely:

$$v_l\big(N_m\big(\phi_n(c-\zeta_m)\big)\big) = f \sum_{\substack{\mathfrak{L}\in\mathbb{P}(O_{mn})\\ \mathfrak{L}|l}} v_{\mathfrak{L}}(c-\zeta_m-\zeta_n), \tag{6}$$

where f is the common order of l modulo m and modulo n (by Corollary 2 to Theorem 2), i.e. f is the order of l modulo mn (since m, n are relatively prime).

Lemma 4. *Let m, n be two relatively prime positive integers. For any prime number l which divides $N_m(\phi_n(\lambda_m)) = N_n(\phi_m(\lambda_n))$, and for any $i \in R_m^*$ and $j \in R_n^*$, there exists a prime ideal of O_{mn} dividing l and $1-\zeta_m^i\sigma_j^{(n)}(\lambda_n)$ (resp. dividing l and $1-\zeta_n^j\sigma_i^{(m)}(\lambda_m)$).*

Proof. By Lemma 3, with $c=1$, there exists a prime ideal $\mathfrak{L}$ of O_{mn} dividing l and $1-\zeta_m-\zeta_n$. Let $k\in R_{mn}^*$ such that $k\equiv -i \pmod m$ and $k\equiv j \pmod n$. Then $\sigma_k^{(mn)}(\mathfrak{L})$ is a prime ideal of O_{mn} which divides l and $1-\zeta_m^{-i}-\zeta_n^j = -\zeta_m^{-i}(1-\zeta_m^i(1-\zeta_n^j))$, i.e. it divides l and $1-\zeta_m^i(1-\zeta_n^j) = 1-\zeta_m^i\sigma_j^{(n)}(\lambda_n)$. By exchange of m and n, a similar result is obtained, with $1-\zeta_n^j\sigma_i^{(m)}(\lambda_m)$ replacing $1-\zeta_m^i\sigma_j^{(n)}(\lambda_n)$. □

Notation. We will use the following notation in the sequel. Given two distinct prime numbers p, q, and the standard reduced residue systems R_p^* modulo p, R_q^* modulo q, R_{pq}^* modulo pq, as defined at the beginning of Section 2, for any $i\in R_p^*$ and any $j\in R_q^*$, we denote by $r(i,j)$ the unique element of R_{pq}^* such that $r(i,j)\equiv i \pmod p$ and $r(i,j)\equiv j \pmod q$.

Proposition 9. *Let p and q be two distinct prime numbers, l a prime number dividing $N_p(\lambda_p^q-1) = N_q(\lambda_q^p-1)$, and f the common order of l modulo p and modulo q.*

(1) *There exist two distinct, conjugate, prime ideals $\mathfrak{L}$ and $\mathfrak{L}'$ of O_{pq} such that $\mathfrak{L}$ divides l and $1-\zeta_q\lambda_p$, and $\mathfrak{L}'$ divides l and $1-\zeta_p\lambda_q$.*

Let $\mathfrak{l} = \mathfrak{L}\cap O_p$ and $\mathfrak{l}' = \mathfrak{L}'\cap O_q$. Then

(2) *$\mathfrak{l}$ (resp. $\mathfrak{l}'$) is a prime ideal of O_p (resp. of O_q), divisible by $\mathfrak{L}$ (resp. $\mathfrak{L}'$), and dividing l and $1-\lambda_p^q$ (resp. dividing l and $1-\lambda_q^p$).*
(3) *$\mathfrak{l}$ (resp. $\mathfrak{l}'$) splits completely in $K_{pq}|K_p$ (resp. in $K_{pq}|K_q$) as a product of $q-1$ (resp. $p-1$) distinct, conjugate, prime ideals of O_{pq}.*
(4) *The prime ideal decomposition of l in $K_{pq}|\mathbb{Q}$ is given by*

$$lO_{pq} = \prod_{k\in C_{pq}(l)} \sigma_k^{(pq)}(\mathfrak{L}) = \prod_{\substack{i\in C_p(l)\\ 1\leqslant j\leqslant q-1}} \sigma_{r(i,j)}^{(pq)}(\mathfrak{L}) = \prod_{\substack{1\leqslant i\leqslant p-1\\ j\in C_q(l)}} \sigma_{r(i,j)}^{(pq)}(\mathfrak{L}') = \prod_{k\in C_{pq}(l)} \sigma_k^{(pq)}(\mathfrak{L}'),$$

where $C_p(l)$ (resp. $C_q(l)$, resp. $C_{pq}(l)$) is a set of coset representatives in R_p^* (resp. R_q^*, resp. R_{pq}^*) of the subgroup generated by the congruence class of l in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ (resp. $(\mathbb{Z}/q\mathbb{Z})^*$, resp. $(\mathbb{Z}/pq\mathbb{Z})^*$).

Proof. (1) The existence of $\mathfrak{L}$ and $\mathfrak{L}'$ follows from Lemma 4, in view of Proposition 2. They are conjugates since they both divide l. They are distinct since $1-\zeta_q\lambda_p$ and $1-\zeta_p\lambda_q$ differ by a unit and are therefore relatively prime. Indeed, $1-\zeta_p\lambda_q-(1-\zeta_q\lambda_p) = \zeta_q-\zeta_p = \zeta_q(1-\zeta_p\zeta_q^{-1}) = \zeta_q(1-\zeta_{pq}^{q-p}) = \zeta_q\sigma_{q-p}^{(pq)}(\lambda_{pq})$, which is a unit of O_{pq}, like $\lambda_{pq} = 1-\zeta_{pq}$ [W, Proposition 2.8].

(2) The fact that $\mathfrak{l}$ (resp. $\mathfrak{l}'$) is a prime ideal of O_p (resp. of O_q), divisible by $\mathfrak{L}$ (resp. $\mathfrak{L}'$), and dividing l results immediately from its definition and the corresponding properties of $\mathfrak{L}$ (resp. $\mathfrak{L}'$). Moreover, as $\mathfrak{L}$ divides $1-\zeta_q\lambda_p$, i.e. $1-\zeta_q\lambda_p\in\mathfrak{L}$, we have $N_{pq,p}(1-\zeta_q\lambda_p)\in\mathfrak{L}\cap O_p = \mathfrak{l}$, where $N_{pq,p}$ is the norm map in $K_{pq}|K_p$, i.e. $\mathfrak{l}$ divides $N_{pq,p}(1-\zeta_q\lambda_p)$. Also, as p and q are distinct

prime numbers, the two field extensions $K_p|\mathbb{Q}$ and $K_q|\mathbb{Q}$ are linearly disjoint, and therefore the Galois groups $Gal(K_{pq}|K_p)$ and $G_q = Gal(K_q|\mathbb{Q})$ are isomorphic, under the isomorphism which assigns to an automorphism $\sigma_j^{(q)}$ of $K_q|\mathbb{Q}$ the automorphism $\sigma_{r(1,j)}^{(pq)}$ of $K_{pq}|\mathbb{Q}$ which leaves K_p fixed, where $r(1,j) \in R_{pq}^*$ such that $r(1,j) \equiv 1 \pmod p$ and $r(1,j) \equiv j \pmod q$. Hence $N_{pq,p}(1-\zeta_q\lambda_p) = \prod_{j=1}^{q-1} \sigma_{r(1,j)}^{(pq)}(1-\zeta_q\lambda_p) = \prod_{j=1}^{q-1}(1-\zeta_q^j\lambda_p) = \frac{1-\lambda_p^q}{1-\lambda_p} = \zeta_p^{-1}(1-\lambda_p^q)$. It follows that $\mathfrak{l}$ divides $1-\lambda_p^q$. Similarly, exchanging p and q, we conclude that $\mathfrak{l}'$ divides $1-\lambda_q^p$.

(3) Since l does not divide pq (by Proposition 6), l is unramified in $K_{pq}|\mathbb{Q}$, and so is the prime ideal above it, $\mathfrak{l}$, in $K_{pq}|K_p$. Moreover, the residue class degree of $\mathfrak{L}$ (resp. $\mathfrak{l}$) over l is equal to the order of l modulo pq (resp. modulo p) [W]. Since the two orders are both equal to f, then, by transitivity, the residue degree of $\mathfrak{L}$ over $\mathfrak{l}$ is equal to 1. It follows that $\mathfrak{l}$ splits completely in $K_{pq}|K_p$, as a product of $[K_{pq}:K_p] = q-1$ distinct prime ideals of O_{pq}, which are conjugates of each other since $K_{pq}|K_p$ is a Galois extension. Similarly, $\mathfrak{l}'$ splits completely in $K_{pq}|K_q$ as a product of $p-1$ distinct, conjugate, prime ideals of O_{pq}, by exchange of p and q.

(4) The decomposition group of the prime ideal $\mathfrak{L}$ in $K_{pq}|\mathbb{Q}$ (resp. $\mathfrak{l}$ in $K_p|\mathbb{Q}$, resp. $\mathfrak{l}'$ in $K_q|\mathbb{Q}$), consisting of the automorphisms of $K_{pq}|\mathbb{Q}$ (resp. of $K_p|\mathbb{Q}$, resp. of $K_q|\mathbb{Q}$) which leave this ideal fixed, is generated by the corresponding Frobenius automorphism $\sigma_l^{(pq)}$ (resp. $\sigma_l^{(p)}$, resp. $\sigma_l^{(q)}$), and is thus isomorphic to the subgroup generated by the congruence class of l in $(\mathbb{Z}/pq\mathbb{Z})^*$ (resp. in $(\mathbb{Z}/p\mathbb{Z})^*$, resp. in $(\mathbb{Z}/q\mathbb{Z})^*$) [W]. Hence $lO_{pq} = \prod_{k\in C_{pq}(l)} \sigma_k^{(pq)}(\mathfrak{L})$ (resp. $lO_p = \prod_{i\in C_p(l)} \sigma_i^{(p)}(\mathfrak{l})$, resp. $lO_q = \prod_{j\in C_q(l)} \sigma_j^{(q)}(\mathfrak{l}')$). Note that, in the prime ideal factorization of lO_{pq}, we can also replace $\mathfrak{L}$ by its conjugate $\mathfrak{L}'$. Moreover, by (3) and (2) above and their proofs, $\mathfrak{l}O_{pq} = \prod_{\sigma\in Gal(K_{pq}|K_p)} \sigma(\mathfrak{L}) = \prod_{j=1}^{q-1} \sigma_{r(1,j)}^{(pq)}(\mathfrak{L})$, and similarly, $\mathfrak{l}'O_{pq} = \prod_{i=1}^{p-1} \sigma_{r(i,1)}^{(pq)}(\mathfrak{L}')$. Hence

$$lO_{pq} = (lO_p)O_{pq} = \prod_{i\in C_p(l)} \sigma_i^{(p)}(\mathfrak{l})O_{pq} = \prod_{i\in C_p(l)} \sigma_{r(i,1)}^{(pq)}(\mathfrak{l}O_{pq}) = \prod_{i\in C_p(l)} \sigma_{r(i,1)}^{(pq)}\left(\prod_{j=1}^{q-1} \sigma_{r(1,j)}^{(pq)}(\mathfrak{L})\right),$$

so that

$$lO_{pq} = \prod_{\substack{i\in C_p(l)\\ 1\leqslant j\leqslant q-1}} \sigma_{r(i,1)}^{(pq)} \circ \sigma_{r(1,j)}^{(pq)}(\mathfrak{L}) = \prod_{\substack{i\in C_p(l)\\ 1\leqslant j\leqslant q-1}} \sigma_{r(i,j)}^{(pq)}(\mathfrak{L}).$$

Similarly,

$$lO_{pq} = (lO_q)O_{pq} = \prod_{j\in C_q(l)} \sigma_{r(1,j)}^{(pq)}\big(\mathfrak{l}'O_{pq}\big) = \prod_{j\in C_q(l)} \sigma_{r(1,j)}^{(pq)}\left(\prod_{i=1}^{p-1} \sigma_{r(i,1)}^{(pq)}\big(\mathfrak{L}'\big)\right)$$
$$= \prod_{\substack{1\leqslant i\leqslant p-1\\ j\in C_q(l)}} \sigma_{r(i,j)}^{(pq)}\big(\mathfrak{L}'\big). \qquad \square$$

Remark 10. For two distinct prime numbers p and q, we have $1-\zeta_q\lambda_p = 1-\zeta_q+\zeta_p\zeta_q$ and $\sigma_{-1}^{(pq)}(1-\zeta_q\lambda_p) = 1-\zeta_q^{-1}+\zeta_p^{-1}\zeta_q^{-1} = \zeta_p^{-1}\zeta_q^{-1}(1-\zeta_p+\zeta_p\zeta_q) = \zeta_p^{-1}\zeta_q^{-1}(1-\zeta_p\lambda_q)$. Thus

$$1-\zeta_p\lambda_q = \zeta_p\zeta_q\sigma_{-1}^{(pq)}(1-\zeta_q\lambda_p). \tag{7}$$

So a prime ideal of O_{pq} divides $1-\zeta_p\lambda_q$ if and only if it divides $\sigma_{-1}^{(pq)}(1-\zeta_q\lambda_p)$. Therefore, in Proposition 9, we may take for prime ideal of O_{pq} dividing l and $1-\zeta_p\lambda_q$ the complex conjugate

$\mathfrak{L}' = \sigma_{-1}^{(pq)}(\mathfrak{L})$ of the prime ideal $\mathfrak{L}$ of O_{pq} dividing l and $1-\zeta_q\lambda_p$. In that case, we get the prime ideals $\mathfrak{l} = \mathfrak{L} \cap O_p$ of O_p dividing l and $1-\lambda_p^q$ and $\mathfrak{l}' = \mathfrak{L}' \cap O_q = \sigma_{-1}^{(pq)}(\mathfrak{L} \cap O_q)$ of O_q dividing l and $1-\lambda_q^p$, so that $\mathfrak{l}$ is the trace of $\mathfrak{L}$ on O_p, while $\mathfrak{l}'$ is the complex conjugate of the trace of $\mathfrak{L}$ on O_q.

Proposition 10. *Let p, q and l be distinct prime numbers, with l dividing $N_p(\lambda_p^q - 1) = N_q(\lambda_q^p - 1)$.*

If there exists more than one prime ideal of O_p dividing l and $1-\lambda_p^q$, then there exist a prime ideal $\mathfrak{L}$ of O_{pq} and two integers $2 \leqslant i \leqslant p-2$ and $2 \leqslant j \leqslant q-2$, with $i \not\equiv l^n \pmod p$ for any integer $n \geqslant 0$, such that $\mathfrak{L}$ divides l and $1-\zeta_q\lambda_p$ and $1-\zeta_q^j\sigma_i^{(p)}(\lambda_p)$.

Similarly, if there exists more than one prime ideal of O_q dividing l and $1-\lambda_q^p$, then there exist a prime ideal $\mathfrak{L}'$ of O_{pq} and two integers $2 \leqslant i \leqslant p-2$ and $2 \leqslant j \leqslant q-2$, with $j \not\equiv l^n \pmod q$ for any integer $n \geqslant 0$, such that $\mathfrak{L}'$ divides l and $1-\zeta_p\lambda_q$ and $1-\zeta_p^i\sigma_j^{(q)}(\lambda_q)$.

Proof. By Proposition 9, there exists a prime ideal $\mathfrak{L}$ of O_{pq} dividing l and $1-\zeta_q\lambda_p$, and then $\mathfrak{l} = \mathfrak{L} \cap O_p$ is a prime ideal of O_p dividing l and $1-\lambda_p^q$. By assumption, there exists another prime ideal of O_p dividing the latter two elements, and it is a conjugate of $\mathfrak{l}$, since it divides l. So there exists an integer $r \in R_p^*$ such that $\sigma_r^{(p)}(\mathfrak{l})$ divides $1-\lambda_p^q$ and $\sigma_r^{(p)}(\mathfrak{l}) \neq \mathfrak{l}$, i.e. $\sigma_r^{(p)}$ does not lie in the decomposition group of $\mathfrak{l}$ in $K_p|\mathbb{Q}$, i.e. the congruence class of r modulo p does not lie in the subgroup generated by that of l in $(\mathbb{Z}/p\mathbb{Z})^*$. Thus, letting i denote the inverse of r modulo p which lies in $\{1, 2, \ldots, p-1\}$, the prime ideal $\mathfrak{l}$ divides $\sigma_i^{(p)}(1-\lambda_p^q) = 1-\sigma_i^{(p)}(\lambda_p)^q$, and $i \not\equiv l^n \pmod p$ for any integer $n \geqslant 0$. Moreover, since $\mathfrak{L}$ divides $\mathfrak{l}$, it also divides $1-\sigma_i^{(p)}(\lambda_p)^q = \prod_{j=0}^{q-1}(1-\zeta_q^j\sigma_i^{(p)}(\lambda_p)) = \zeta_p^i\prod_{j=1}^{q-1}(1-\zeta_q^j\sigma_i^{(p)}(\lambda_p))$, i.e. there exists an integer $1 \leqslant j \leqslant q-1$ such that $\mathfrak{L}$ divides $1-\zeta_q^j\sigma_i^{(p)}(\lambda_p)$. Note also that, since $i \not\equiv l^n \pmod p$ for all $n \geqslant 0$, then $i \neq 1$, so that $2 \leqslant i \leqslant p-1$.

Furthermore, if $j = 1$, then $\mathfrak{L}$ divides $1-\zeta_q\lambda_p$ and $1-\zeta_q\sigma_i^{(p)}(\lambda_p)$, so $\mathfrak{L}$ divides their difference $\zeta_q(\sigma_i^{(p)}(\lambda_p) - \lambda_p) = \zeta_q(\zeta_p - \zeta_p^i) = \zeta_q\zeta_p(1-\zeta_p^{i-1}) = \zeta_p\zeta_q\sigma_{i-1}^{(p)}(\lambda_p)$, i.e. $\mathfrak{L}$ divides $\sigma_{i-1}^{(p)}(\lambda_p)$, which is impossible, since $\sigma_{i-1}^{(p)}(\lambda_p)$ divides p and $\mathfrak{L}$ divides l while p is relatively prime to l, by Proposition 6. Thus $j \neq 1$. Also, if $j = q-1$, then $\mathfrak{L}$ divides $1-\zeta_q\lambda_p$ and $1-\zeta_q^{q-1}\sigma_i^{(p)}(\lambda_p)$, so $\mathfrak{L}$ divides $1-\zeta_q\lambda_p + \zeta_q(1-\zeta_q^{q-1}\sigma_i^{(p)}(\lambda_p)) = \zeta_p\zeta_q + \zeta_p^i = \zeta_p\zeta_q(1+\zeta_p^{i-1}\zeta_q^{-1}) = \zeta_p\zeta_q(1+\zeta_{pq}^{q(i-1)-p}) = \zeta_p\zeta_q\sigma_{q(i-1)-p}^{(pq)}(1+\zeta_{pq}) = \zeta_p\zeta_q\sigma_{q(i-1)-p}^{(pq)}(u_{pq,2})$, where $u_{pq,2}$ is the cyclotomic unit $\frac{1-\zeta_{pq}^2}{1-\zeta_{pq}} = 1+\zeta_{pq}$, so that $\mathfrak{L}$ divides a unit, which is impossible. Thus $j \neq q-1$. Therefore $2 \leqslant j \leqslant q-2$.

Similarly, if $i = p-1$, then $\mathfrak{L}$ divides $1-\zeta_q^j\sigma_{p-1}^{(p)}(\lambda_p)$ and $1-\zeta_q\lambda_p$, so $\mathfrak{L}$ divides their difference $\zeta_q\lambda_p - \zeta_q^j\sigma_{p-1}^{(p)}(\lambda_p) = \zeta_q\lambda_p(1-\zeta_q^{j-1}u_{p,p-1})$, where $u_{p,p-1} = \frac{\sigma_{p-1}^{(p)}(\lambda_p)}{\lambda_p} = \frac{1-\zeta_p^{-1}}{1-\zeta_p} = -\zeta_p^{-1}$. Thus $\mathfrak{L}$ divides $\zeta_q\lambda_p(1+\zeta_q^{j-1}\zeta_p^{-1}) = \zeta_q\lambda_p(1+\zeta_{pq}^{p(j-1)-q}) = \zeta_q\lambda_p\sigma_{p(j-1)-q}^{(pq)}(1+\zeta_{pq}) = \zeta_q\lambda_p\sigma_{p(j-1)-q}^{(pq)}(u_{pq,2})$, which is impossible, since $\zeta_q\lambda_p\sigma_{p(j-1)-q}^{(pq)}(u_{pq,2})$ is an associate of λ_p (note that $p(j-1)-q$ is relatively prime to pq, since $2 \leqslant j \leqslant q-2$). Thus $i \neq p-1$. Therefore $2 \leqslant i \leqslant p-2$.

The remaining part is obtained by exchanging p and q. □

Corollary 1. *Let p be a prime number $\geqslant 5$. For any prime number l dividing $N_p(\lambda_p^3 - 1) = N_3(\lambda_3^p - 1)$, we have $l \equiv 1 \pmod{3p}$, and there exists a unique prime ideal $\mathfrak{l}$ of O_p (resp. $\mathfrak{l}'$ of O_3) dividing l and $1-\lambda_p^3$ (resp. dividing l and $1-\lambda_3^p$).*

Proof. The congruence $l \equiv 1 \pmod{3p}$ was proved in Corollary 1 to Proposition 8. The existence of $\mathfrak{l}$ (resp. $\mathfrak{l}'$) results from Lemma 2, and its uniqueness follows from Proposition 10, since $p \geqslant 5$ and $q = 3$ are distinct odd primes and there are no integers $2 \leqslant j \leqslant q-2$, so that l and $1-\lambda_p^3$ (resp. l and $1-\lambda_3^p$) cannot have more than one prime ideal divisor in O_p (resp. O_3).

Note that the uniqueness of $\mathfrak{l}'$ was also proved in the corollary following Remark 8. □

Corollary 2. *Let p be a prime number $\geqslant 5$, and let*

$$N_p\big(\lambda_p^3-1\big)=N_3\big(\lambda_3^p-1\big)=\prod_{i=1}^{r} l_i^{h_i}$$

be the rational prime factorization of the norm, where $l_1,\dots,l_r$ are distinct prime numbers and $h_1,\dots,h_r$ are positive integers. Then, for every $1\leqslant i\leqslant r$, there exists a unique prime ideal $\mathfrak{l}_i$ of O_p (resp. $\mathfrak{l}'_i$ of O_3) dividing l_i and $1-\lambda_p^3$ (resp. dividing l_i and $1-\lambda_3^p$), and we have the similar prime ideal factorizations

$$\big(1-\lambda_p^3\big)O_p=\prod_{i=1}^{r}\mathfrak{l}_i^{h_i},\qquad \big(1-\lambda_3^p\big)O_3=\prod_{i=1}^{r}\mathfrak{l}_i'^{h_i}.$$

Proof. The existence and uniqueness, for every i, of the prime ideal $\mathfrak{l}_i$ (resp. $\mathfrak{l}'_i$), and the fact that the common order of every l_i modulo p and modulo q is $f_i=1$ all follow from the previous corollary. The prime ideal factorizations of $(1-\lambda_p^3)O_p$ and $(1-\lambda_3^p)O_3$ follow from Theorem 6, since for every i, we have $m_i=h_i$ and $\mathfrak{l}_{i,1}=\cdots=\mathfrak{l}_{i,m_i}=\mathfrak{l}_i$, as the only prime ideal of O_p dividing $1-\lambda_p^3$ and l_i is $\mathfrak{l}_i$, and similarly $\mathfrak{l}'_{i,1}=\cdots=\mathfrak{l}'_{i,m_i}=\mathfrak{l}'_i$. □

Examples. By Remark 3, for any positive integers m, n and any $c\in\mathbb{Z}$, the norm $N_m(\phi_n(c-\zeta_m))$ can be expressed as the resultant of two polynomials, namely

$$N_m\big(\phi_n(c-\zeta_m)\big)=N_n\big(\phi_m(c-\zeta_n)\big)=R\big(\phi_m(X),\phi_n(c-X)\big)=R\big(\phi_n(X),\phi_m(c-X)\big).$$

In particular, in view of Proposition 2, for any prime numbers p, q,

$$N_p\big(\lambda_p^q-1\big)=N_q\big(\lambda_q^p-1\big)=R\big(\phi_p(X),\phi_q(1-X)\big)=R\big(\phi_q(X),\phi_p(1-X)\big).$$

Using these expressions, and the PARI/GP calculator, we computed $N_p(\lambda_p^q-1)$ for 218 pairs of distinct primes (p,q) such that $3\leqslant p\leqslant 53$ and $2\leqslant q\leqslant M(p)$, where $M(p)$ is an upper bound depending on the difficulty of factoring some large numbers obtained as norms. Thus $M(3)=173$, $M(5)=127$, $M(7)=101$, $M(11)=73$, $M(13)=67$, $M(17)=M(19)=31$, $M(23)=37$, $M(29)=M(31)=23$, $M(37)=13$, $M(41)=19$, $M(43)=13$, $M(47)=23$, and $M(53)=19$.

All but three of the resulting values of $N_p(\lambda_p^q-1)$ were found to be square-free, i.e. to satisfy $N_p(\lambda_p^q-1)=\prod_{i=1}^{r} l_i$, where $l_1,\dots,l_r$ are distinct prime numbers. This implies, by Corollary 2 to Proposition 7, that $l_i\equiv 1 \pmod{pq}$ for $1\leqslant i\leqslant r$, and, by Theorem 6, that for every i, there exists a unique prime ideal $\mathfrak{l}_i$ of O_p (resp. $\mathfrak{l}'_i$ of O_q) dividing l_i and $1-\lambda_p^q$ (resp. dividing l_i and $1-\lambda_q^p$), and we have the prime ideal factorization $(1-\lambda_p^q)O_p=\prod_{i=1}^{r}\mathfrak{l}_i$ (resp. $(1-\lambda_q^p)O_q=\prod_{i=1}^{r}\mathfrak{l}'_i$), since in the notations of Theorem 6, $f_i=m_i=h_i=1$ for $1\leqslant i\leqslant r$.

The exceptions are $N_5(\lambda_5^{43}-1)$ which has the factor 431^2, and $N_{11}(\lambda_{11}^{31}-1)$ which has the factor 683^2, and $N_{13}(\lambda_{13}^{67}-1)$ which has the factor 5227^2. However, in all these exceptions, as in the square-free cases, the prime factors of $N_p(\lambda_p^q-1)$ are all $\equiv 1 \pmod{pq}$. Moreover, in the first exception, we found the prime ideal factorization of $(1-\lambda_5^{43})O_5$ in O_5 and of $(1-\lambda_{43}^5)O_{43}$ in O_{43}. Indeed, $N_5(\lambda_5^{43}-1)=N_{43}(\lambda_{43}^5-1)=l_1^2l_2l_3$, where $l_1=431$, $l_2=462\,563\,041$ and $l_3=13\,254\,765\,131\,080\,801$ are prime numbers $\equiv 1 \pmod{5\times 43}$. Then $(1-\lambda_5^{43})O_5=\mathfrak{l}_{1,1}\mathfrak{l}_{1,2}\mathfrak{l}_2\mathfrak{l}_3$, where $\mathfrak{l}_{1,1}=l_1O_5+(26+\zeta_5)O_5$ and $\mathfrak{l}_{1,2}=l_1O_5+(-95+\zeta_5)O_5$ are distinct, conjugate prime ideals of O_5, the only ones dividing l_1 and $1-\lambda_5^{43}$, i.e. satisfying $l_1O_5+(1-\lambda_5^{43})O_5=\mathfrak{l}_{1,1}\mathfrak{l}_{1,2}$, while $\mathfrak{l}_2=l_2O_5+(1-\lambda_5^{43})O_5=l_2O_5+(131\,372\,863+\zeta_5)O_5$ is the only prime ideal of O_5 dividing l_2 and

$1-\lambda_5^{43}$, and $\mathfrak{l}_3 = l_3 O_5 + (1-\lambda_5^{43})O_5 = l_3 O_5 + (-350\,923\,649\,835\,305 + \zeta_5)O_5$ is the only prime ideal of O_5 dividing l_3 and $1-\lambda_5^{43}$. Similarly, $(1-\lambda_{43}^5)O_{43} = \mathfrak{l}'_{1,1}\mathfrak{l}'_{1,2}\mathfrak{l}'_2\mathfrak{l}'_3$, where $\mathfrak{l}'_{1,1} = l_1 O_{43} + (-27+\zeta_{43})O_{43}$ and $\mathfrak{l}'_{1,2} = l_1 O_{43} + (94+\zeta_{43})O_{43}$ are distinct, conjugate prime ideals of O_{43}, the only ones dividing l_1 and $1-\lambda_{43}^5$, i.e. satisfying $l_1 O_{43} + (1-\lambda_{43}^5)O_{43} = \mathfrak{l}'_{1,1}\mathfrak{l}'_{1,2}$, while $\mathfrak{l}'_2 = l_2 O_{43} + (1-\lambda_{43}^5)O_{43} = l_2 O_{43} + (-131\,372\,864 + \zeta_{43})O_{43}$ is the only prime ideal of O_{43} dividing l_2 and $1-\lambda_{43}^5$, and $\mathfrak{l}'_3 = l_3 O_{43} + (1-\lambda_{43}^5)O_{43} = l_3 O_{43} + (350\,923\,649\,835\,304 + \zeta_{43})O_{43}$ is the only prime ideal of O_{43} dividing l_3 and $1-\lambda_{43}^5$.

Acknowledgment

I would like to thank the referee, whose comments and suggestions helped improve the original version of the paper.

References

[AT] E. Artin, J. Tate, Class Field Theory, Benjamin, New York, 1967.
[H] H. Hasse, Number Theory, Springer, New York, 1980.
[He] C. Helou, A reciprocity relation between some cyclotomic integers, in: Number Theory for the Millennium, II, Urbana, IL, 2000, A K Peters, Nattick, MA, 2002, pp. 167–174.
[IR] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second ed., Springer, New York, 1990.
[L] S. Lang, Algebra, third ed., Springer, New York, 2002.
[W] L. Washington, Introduction to Cyclotomic Fields, second ed., Springer, New York, 1997.
[ZS] O. Zariski, P. Samuel, Commutative Algebra, vol. 1, Springer, New York, 1975.